



www.archive.org
415.561.6767
415.840-0391 e-fax

Internet Archive
300 Funston Avenue
San Francisco, CA 94118

AFFIDAVIT OF CHRISTOPHER BUTLER

1. I am the Office Manager at the Internet Archive, located in San Francisco, California. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to surf more than 400 billion pages stored in the Internet Archive's web archive. Visitors to the Wayback Machine can search archives by URL (i.e., a website address). If archived records for a URL are available, the visitor will be presented with a list of available dates. The visitor may select one of those dates, and then begin surfing on an archived version of the Web. The links on the archived files, when served by the Wayback Machine, point to other archived files (whether HTML pages or images). If a visitor clicks on a link on an archived page, the Wayback Machine will serve the archived file with the closest available date to the page upon which the link appeared and was clicked.

4. The archived data made viewable and browseable by the Wayback Machine is compiled using software programs known as crawlers, which surf the Web and automatically store copies of web files, preserving these files as they exist at the point of time of capture.

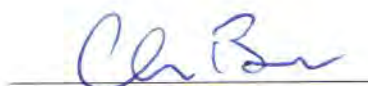
5. The Internet Archive assigns a URL on its site to the archived files in the format [http://web.archive.org/web/\[Year in yyyy\]\[Month in mm\]\[Day in dd\]\[Time code in hh:mm:ss\]/\[Archived URL\]](http://web.archive.org/web/[Year in yyyy][Month in mm][Day in dd][Time code in hh:mm:ss]/[Archived URL]). Thus, the Internet Archive URL <http://web.archive.org/web/19970126045828/http://www.archive.org/> would be the URL for the record of the Internet Archive home page HTML file (<http://www.archive.org/>) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). A web browser may be set such that a printout from it will display the URL of a web page in the printout's footer.

6. The date assigned by the Internet Archive applies to the HTML file but not to image files linked therein. Thus images that appear on a page may not have been archived on the same date as the HTML file. Likewise, if a website is designed with "frames," the date assigned by the Internet Archive applies to the frameset as a whole, and not the individual pages within each frame.

6. Attached hereto as Exhibit A are true and accurate electronic copies of printouts of the Internet Archive's records of the HTML and PDF files for the URLs and the dates specified in the footer of the printout (for HTML) or attached coversheet (for PDF).

7. I declare under penalty of perjury that the foregoing is true and correct.

DATE: 9/29/15



Christopher Butler

EXHIBIT A



Home Products Forum Company Support Downloads Developers Purchase

Enter Your Search:

[Click Here To Search Our Forums](#)

Top 10 NetRemote Plug-ins

[ZoomDriver-1](#)

[View All >>](#)

Newest NetRemote Config Files

Thumbnail	Downloads
	505
	473
	175
	198
	384

[View All >>](#)

Join Our Mailing List

Receive new version announcements and special offers.

Your email address

Subscribe Un-Subscribe

Promixis does not market, rent, or sell its customer email list to ANY outside parties. The Promixis Newsletter will only be sent to you with your consent. All emails we send you will contain unsubscribe information, and you may opt-out of future emails at any time.

Products - NETREMOTE



NetRemote LE
\$19.99

NetRemote IR
\$19.99
Coming Soon

NetRemote Pro
\$29.99
Coming Soon

NetRemote from Promixis is the ultimate in 2 way remote control using your Pocket PC or any Windows computer. Unleash your digital media library and control your computer and home automation systems wirelessly! Using NetRemote and your WiFi enabled Pocket PC or any networked Windows computer, you will have full control of your digital media from **anywhere** in your house. With NetRemote IR, you can replace all of your remote controls with a Pocket PC.

Digital DJ:
 Browse your music by artist, genre, playlist, title or even by album cover, adjust the volume, and let the music play. Use NetRemote for your next party and let your guests play DJ by passing the PocketPC around. NetRemote is incredibly easy and fun, and once you use it, you'll never put it down.

Total Remote Control:
 Toss your remotes away- all you need is your PocketPC and NetRemote and you can control your home theater, TV, stereo or any other IR enabled device using the IR signal transmitting and learning in the NetRemote IR and NetRemote Pro versions. Take advantage of the large library of Pronto CCF files available on the internet.

Multimedia Maestro:
 Using NetRemote and your favorite media player, control your A/V presentations, slideshows, and digital video using your PocketPC. It's easy!

Home Automation:
 NetRemote can control your home automation system when used conjunction with Girder, HomeSeer and other 3rd party applications. NetRemote allows 2 way communication with any TCP/IP device and can control serial and IR devices directly using the Global Cache device.

Sophisticated Custom Controls
 NetRemote Pro provides a sophisticated environment for custom screens and controls using its built in scripting language. Display data from a wide variety of sources including weather and TV channel listings.

NetRemote comes in three versions providing expanded levels of control and sophistication. See the chart below for a comparison of NetRemote LE, IR, and PRO.

Feature	NetRemote LE: \$19.99	NetRemote IR: \$19.99	NetRemote Pro: \$29.99
	Remote-control your media player anywhere in your house via wi-fi! Browse your media library and cover art. Select songs and playlists.	Throw away your remotes and control your IR devices from Netremote. Use any Pronto™ CCF file or design your own.	The most complete and flexible two-way control for the PocketPC. Period. Go for total control with NetRemote Pro.
Use Your PocketPC as a remote control.	X	X	X
Two way control of J. River Media Center	X		X
Two way control of iTunes	Coming Soon		Coming Soon
Two way control of Windows Media Player	Coming Soon		X

NetRemote Skins
 Personalize your NetRemote!
[View and download skins here!](#)

Feeling creative? **Upload** your NetRemote skin for all the world to see. NetRemote uses Pronto CCF's for full creativity and customization.

Platform & Device Support
 NetRemote runs on most Pocket PC 2002 and 2003 devices using the Microsoft Windows Mobile OS. This includes popular handheld devices such as the HP iPaq and Dell Axim lines.

Also note, to utilize the wireless internet/ wi-fi functions of NetRemote, your PocketPC device must be enabled for wi-fi connectivity.

Screenshots
[Click here](#) to see NetRemote in action!

- Documentation & Support**
- [NetRemote LE Installation Guide](#)
 - [NetRemote LE Setup Guide](#)
 - [NetRemote LE Network Configuration Guide](#)
 - [NetRemote Forum](#)
 - [Downloads](#)

EXHIBIT A

Loads Pronto Pro Files	X	X	X
Loads Marantz RC9200 Files	X	X	X
Transmits and Learns Infrared (IR) From Pocket PC		X	X
Sends Infrared (IR) to PC IR Server			X
Two way control of Zoom Player			X
Two way control of Girder			X
Embedded Web Browser			X
Two way control of GlobalCache device			X
Wake-On-Lan support (turns computer on remotely)			X
	BUY NOW	Coming Soon	Coming Soon

NetRemote- unleash your digital media library!

©2004 Promixis, LLC
 Privacy Policy | Website Terms of Use

[Web-Stat hit counters](#)

EXHIBIT A

http://web.archive.org/web/20050120005959/http://promixis.com/pdfs/NetRemote_LE_Installation_Guide.pdf

NetRemote LE Installation Guide for J. River Media Center

1. Download NetRemote.

Download NetRemote LE from [Promixis](#) and save the file on your computer (your Desktop is an easy place). You may delete the installation program when finished.

2. Install NetRemote.

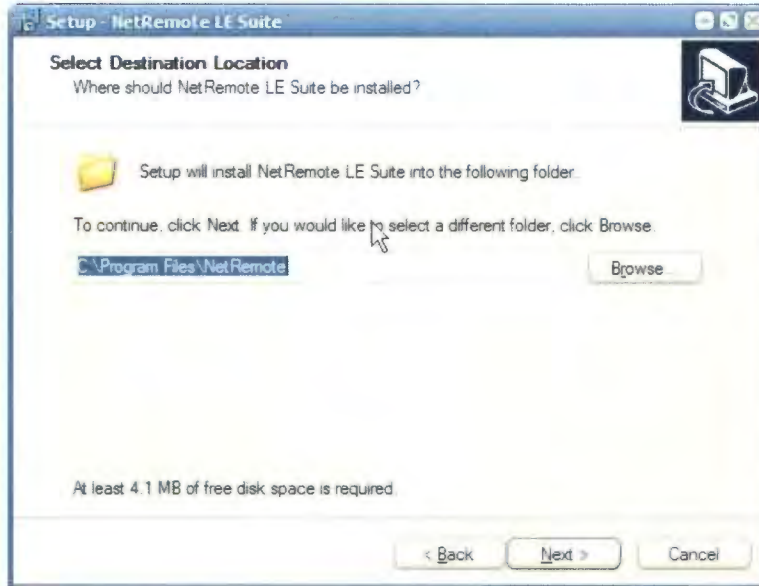
NetRemote is installed by running the file you just downloaded. Double click the file to start the installation process. The first screen is the NetRemote license agreement. Please read this carefully. Each license allows you to install NetRemote on 2 different personal computers (PC's) or pocket PC's (PPC).



Next, you will choose which version of NetRemote to install. If ActiveSync is not detected, only the option for installing the Windows version will be selectable.

3. NetRemote for Windows (98,Me,XP,2000,2003)

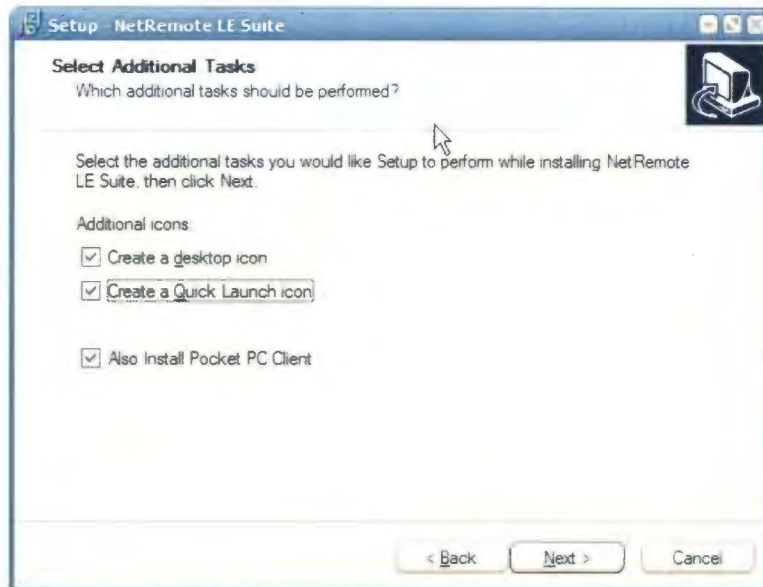
The destination folder is where the NetRemote program is installed on your hard drive. We suggest you use the default folder as shown below. Click **Next** to continue.



Next, select the Start Menu folder. Click **Next** to continue.

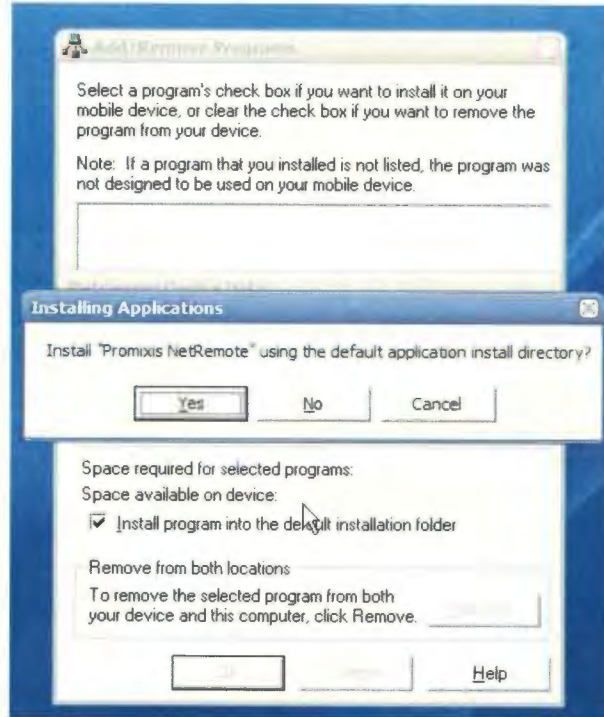


After NetRemote is installed, you can then select to have Short Cuts created on the Desktop and Quick Launch bars. Select the options you want. If you have an ActiveSync connection, the option to install the Pocket PC Client is available. Click **Next** to continue

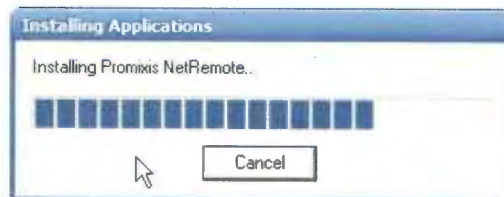


4. NetRemote for the PPC (2002, 2003)

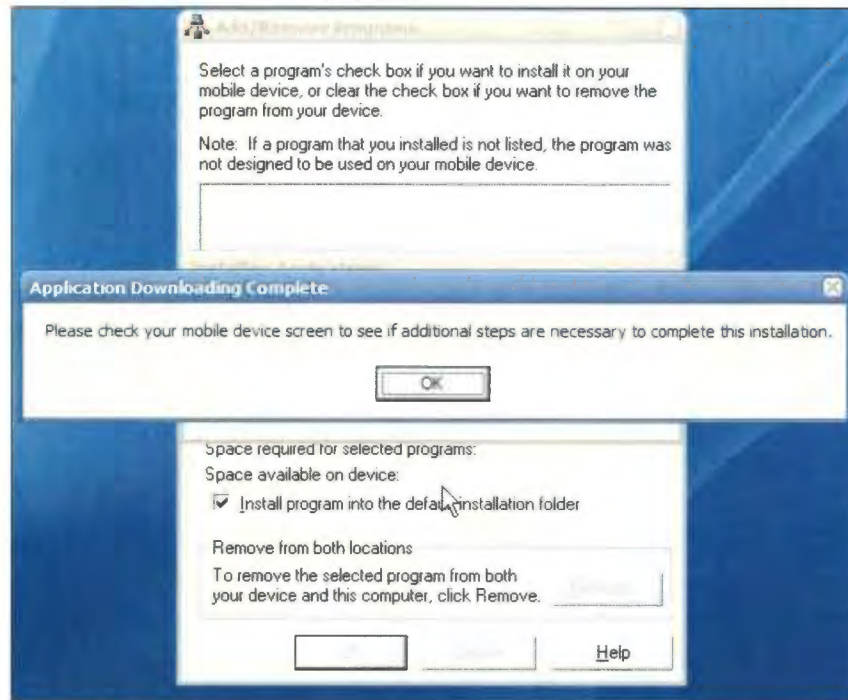
The option for installing the PPC version is only available on computers that have ActiveSync installed. After installing the PPC version, if your PPC is connected, ActiveSync displays the screen below.



Click **Yes** to install in the default directory (suggested). ActiveSync will then display a progress bar as the application is installed.

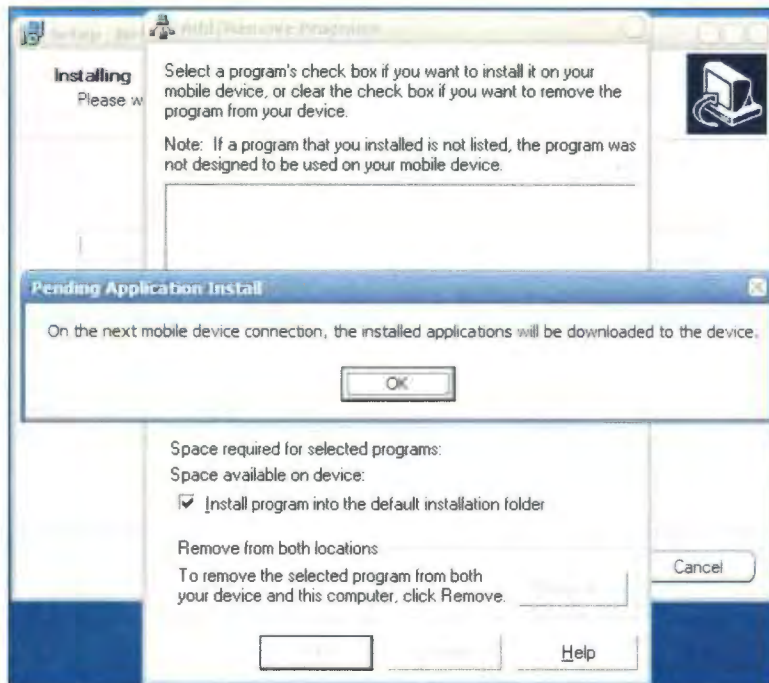


When the installation is completed, ActiveSync will display.

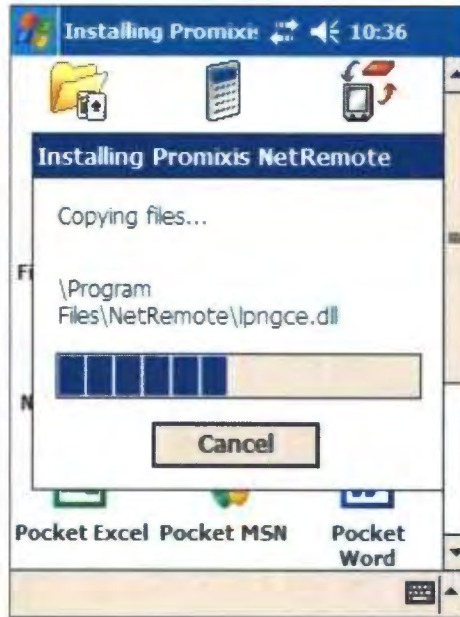


Click **OK** to continue.

If your PPC is not connected to your computer then ActiveSync will show the screen below.



Click **OK** to continue. When you connect your PPC, NetRemote will be installed as described above. See your PPC device and follow the instructions on the screen.



5. Final Steps

Before the installation ends, you will have the option to start Media Center (if installed on this PC) and to launch NetRemote (if installed on this PC). It is recommended you start Media Center prior to starting NetRemote so that NetRemote can automatically configure the network settings for you.

Please see the **NetRemote LE Network Configuration Guide** for setting up NetRemote on your network.

EXHIBIT A

http://web.archive.org/web/20050119225451/http://promixis.com/pdfs/NetRemote_LE_Setup_Guide.pdf

NetRemote LE Setup Guide

This guide explains how to setup the NetRemote MediaBridge plugin for J. River's Media Center. For problems with network configuration, please see the NetRemote LE Network Configuration Guide.

Start either the NetRemote Windows or Pocket PC client.

Open the Properties Page.

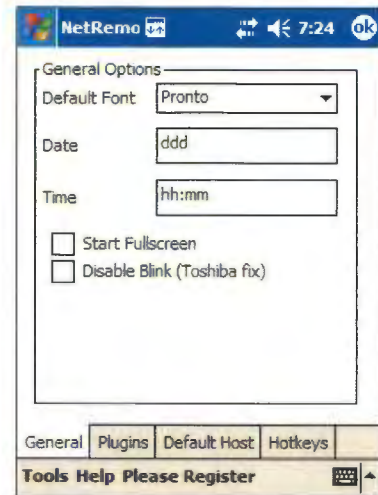
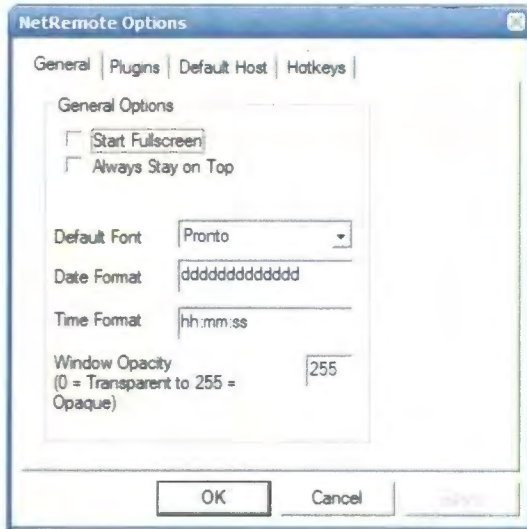
For the Windows client, click File/ Properties.



For the Pocket PC client, tap Tools/ Properties.



General Tab



Start Full Screen sets NetRemote to start up full screen.

Always On Top Option (Windows Client Only) keeps NetRemote always visible.

Default Font sets the font used to draw buttons and labels. In most instances, this should not be changed.

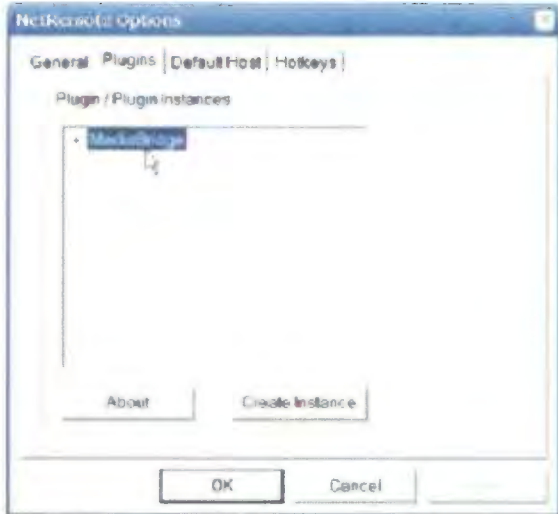
Date Format controls how the day of the week is displayed. Each “d” represents one letter, ie. “ddd” for Monday will show “Mon”.

Time Format controls how the time is displayed. “hh:mm:ss” will show the hour, minute, second.

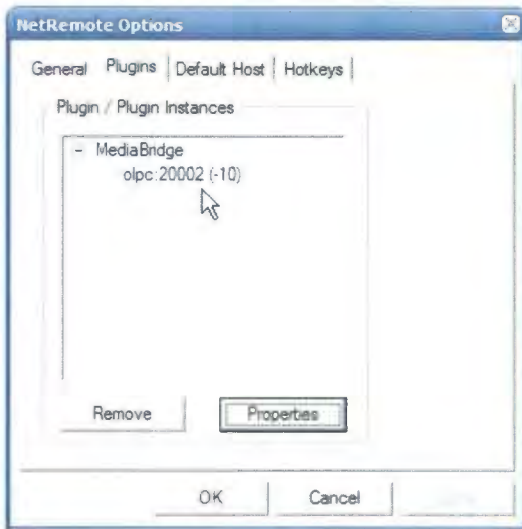
Window Opacity (Windows Client Only) is used to make the NetRemote window transparent. Values less than 200 are not recommended. This setting is useful with the Always On Top option.

Plugins Tab

On this tab, the list of NetRemote plugins are displayed. In the LE or IR editions of NetRemote, this is limited to the MediaBridge and IR plugins respectively.



Each plugin can have multiple "instances". This allows NetRemote to communicate with more than one server. For instance, you could have Media Center running on multiple computers. Click on the plus sign to view a list of connections. The screen will change as shown below.



To change the configuration of an instance of the plugin, click on it to highlight it and then click on Properties. This will bring up the next dialog box.

MediaBridge Properties

JRMC Plugin

Host: HSMPC

Port: 20002

Default Img Size: XLarge

Control Font: Verdana

Library Root:

Use "Add To Playlist" Menu

Show Playing Now In Tree

Cancel Help OK

NetRemo

Host:

Port: 20002

Default Img Size: Medium

Control Font:

Library Root:

Use "Add To Playlist" Menu

Show Playing Now In Tree

Cancel Help OK

Tools Help Please Register

Host specifies the computer that this instance of the plugin connects to. This can be the computer name or the IP address.

Port specifies the port that NetRemote uses.

Default Img Size is the size of cover art images that NetRemote will use. On windows clients use Large or XLarge. On Pocket PC devices, you may want to use Medium or smaller. This is done for performance reasons.

Control Font specifies the font used to display the media library and playing now lists.

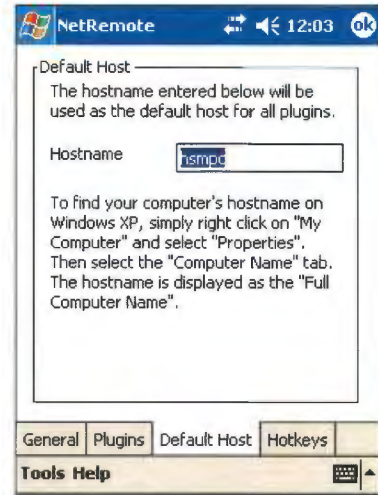
Library Root is used with Media Center. It specifies where in the Media Library that NetRemote should begin displaying from.

Use "Add to Playlist" Menu adds the option to add songs to a playlist in Media Center. This option may cause performance problems on slower Pocket PC clients.

Show Playing Now in Tree will display the currently playing songs in the Media Library tree.

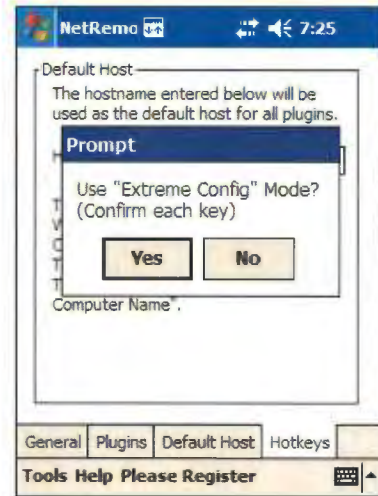
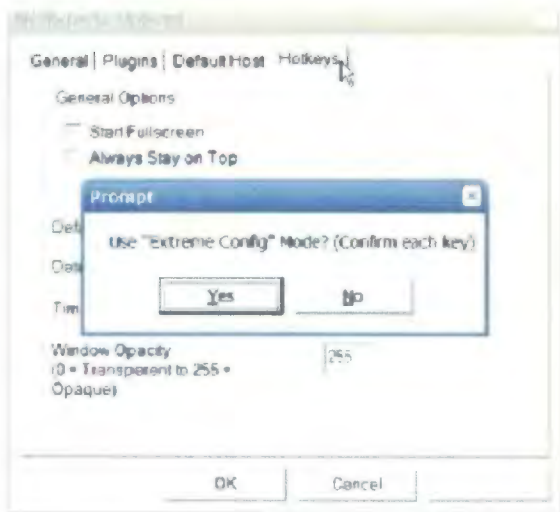
Press OK to save you changes.

Default Host Tab



Default Host specifies with host computer NetRemote should connect with first. Enter either the computer name or IP address in this box. Click OK when done.

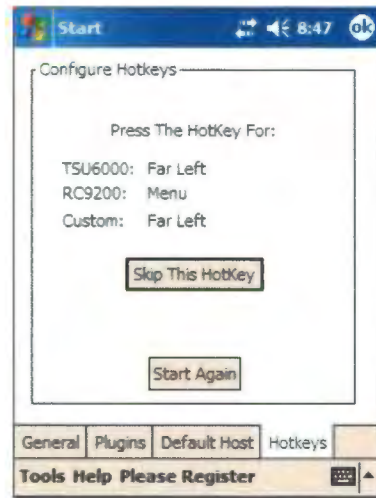
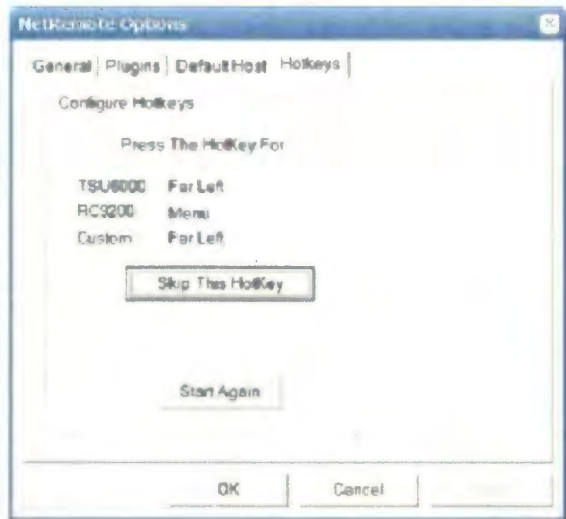
HotKeys Tab



The Extreme Config mode is usually not necessary. Click NO unless you are having problems configuring your device.

EXHIBIT A

NetRemote will then configure all of the HotKeys found on the Pronto (or similar) remote controls. The commands these keys are linked to are specified in the current CCF file.



Configuring J. River Media Center for Album Covers View

NetRemote will display all of your albums by cover art, as shown below. This requires you to create a new View Scheme in JRMC.



Adding the album cover art View Scheme to JRM:

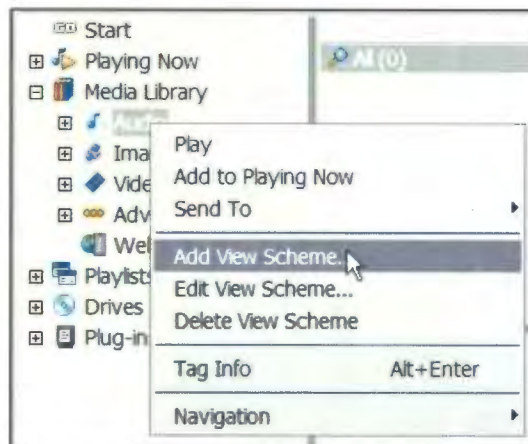
1. Start JRM.
2. Open up the Media Library tree by clicking on the plus sign.



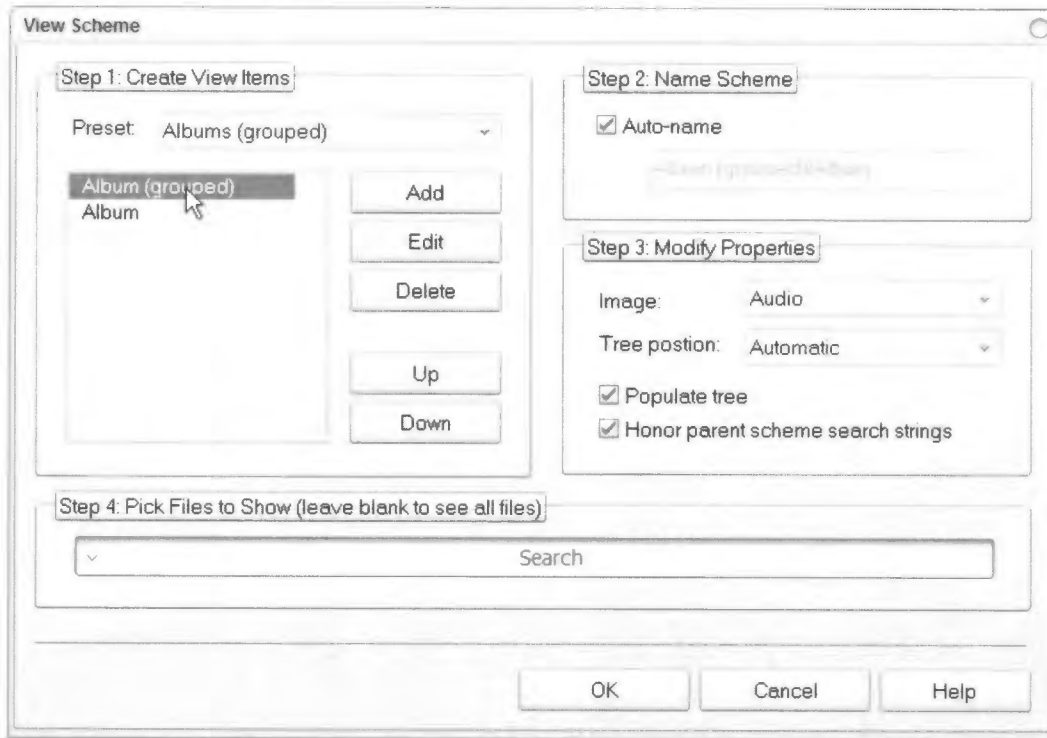
3. Right Click Audio.



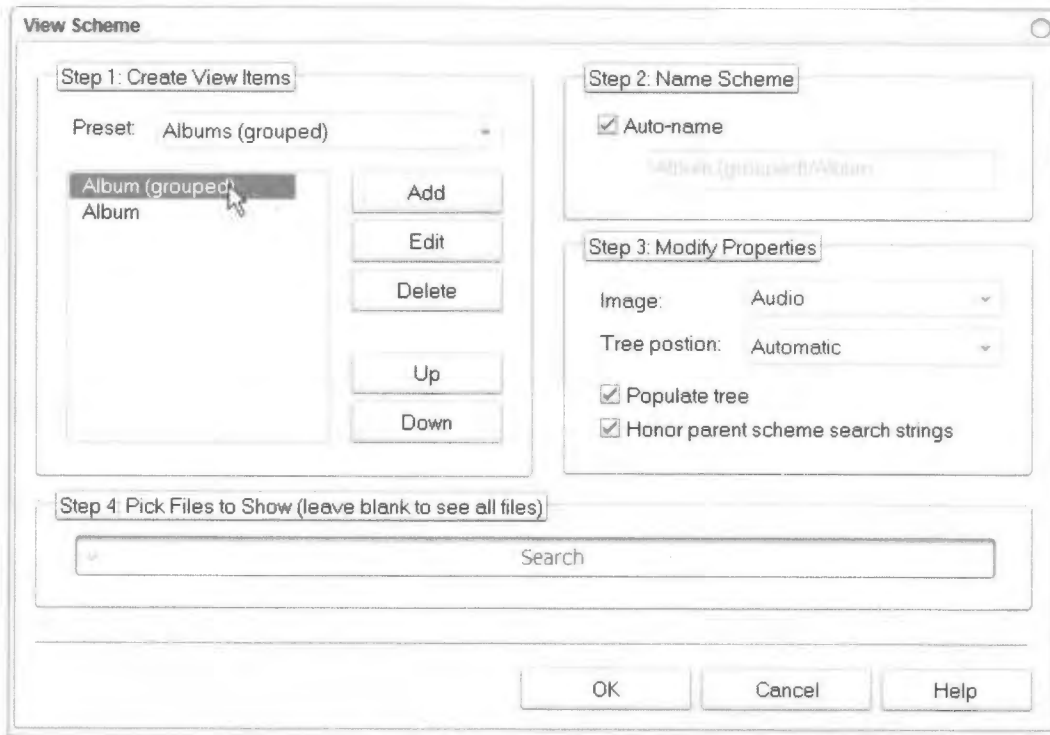
4. Click Add View Scheme.



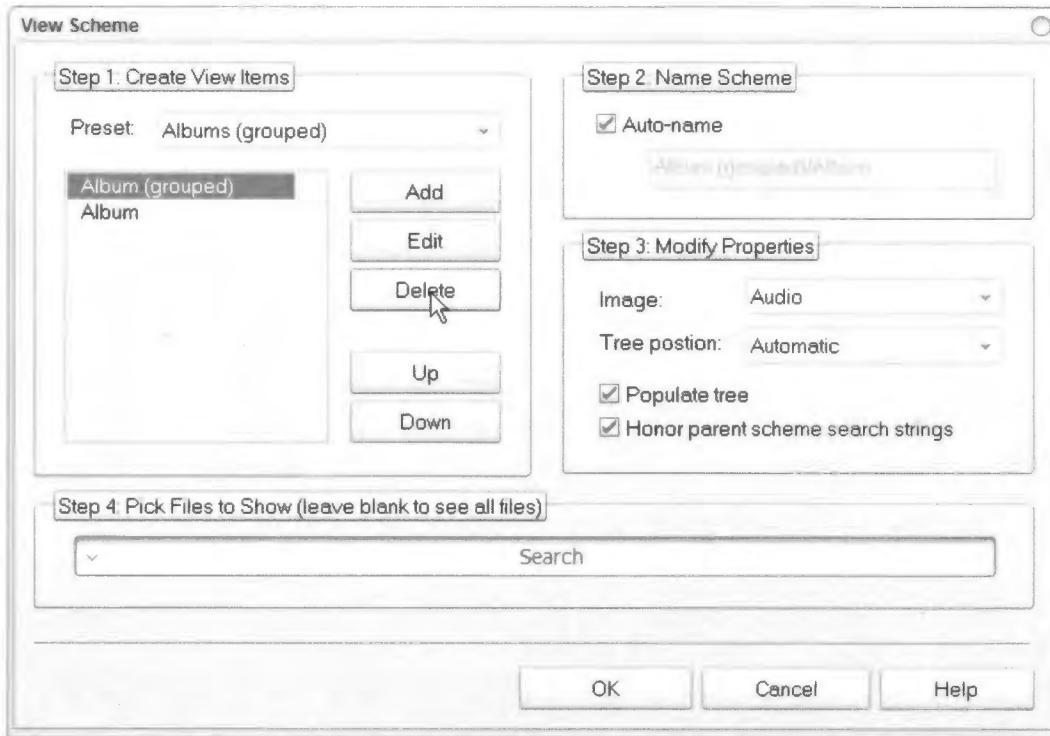
5. Select Album (Grouped).



6. Select the Album (Grouped) text.



7. Click Delete.



8. Click OK.

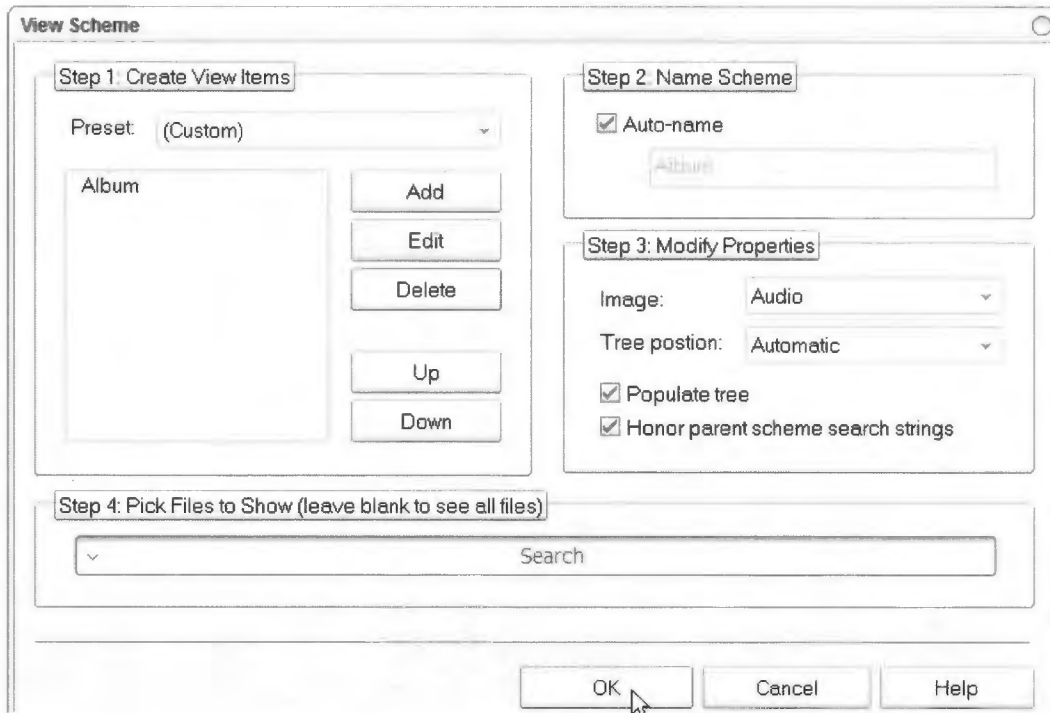


EXHIBIT A

http://web.archive.org/web/20050119225826/http://promixis.com/pdfs/NetRemote_LE_Network_Configuration_Guide.pdf

NetRemote LE Network Configuration Guide

Automatic Network Configuration

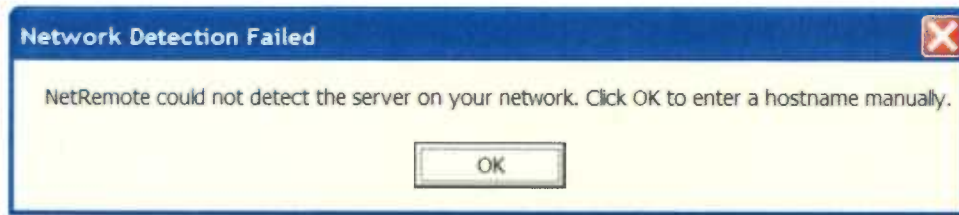
NetRemote works by “talking” to J. River Media Center (JRMCM) over your network. It works with both wired and wireless networks. NetRemote is designed to automatically configure and connect to any computers on your network running JRMCM. You must have your devices already connected to your network before configuring NetRemote.

Start J. River Media Center on your computer.

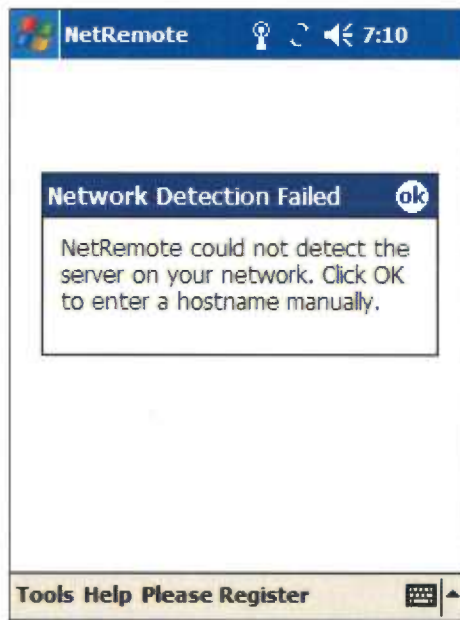
Start NetRemote (either the Windows or Pocket PC version). NetRemote will take a few seconds to examine your network and try and find any computer that is running JRMCM. After NetRemote has completed this step, you will see a screen similar to below, depending on what Media Center is playing.



If NetRemote cannot connect to JRMC you will see this message on the Windows Client.



On the Pocket PC client you will see this message.



Proceed to the Manual Configuration guide below.

Manual Network Configuration

In some instances, depending on your network configuration and security settings, automatic configuration may not work. In this case, follow the steps below.

Step 1. Configure J. River Media Center (JRMC)

Start JRMC. Open up the Options dialog by pressing Ctrl-O or from the Tools Menu.

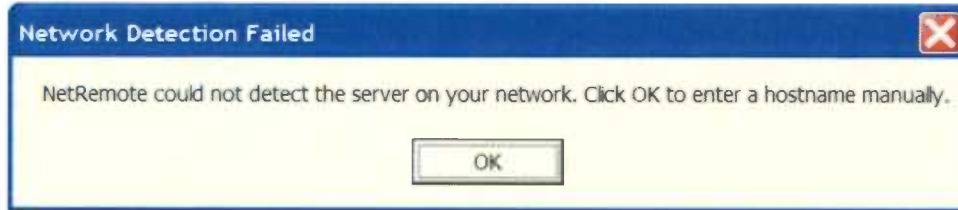


The Options dialog is then displayed. Select Startup. Under actions, check the Run Remote Server box and specify the port address. In most installations the default port of 20002 will work fine. Click OK. You are now finished setting up JRMC. Leave JRMC running.

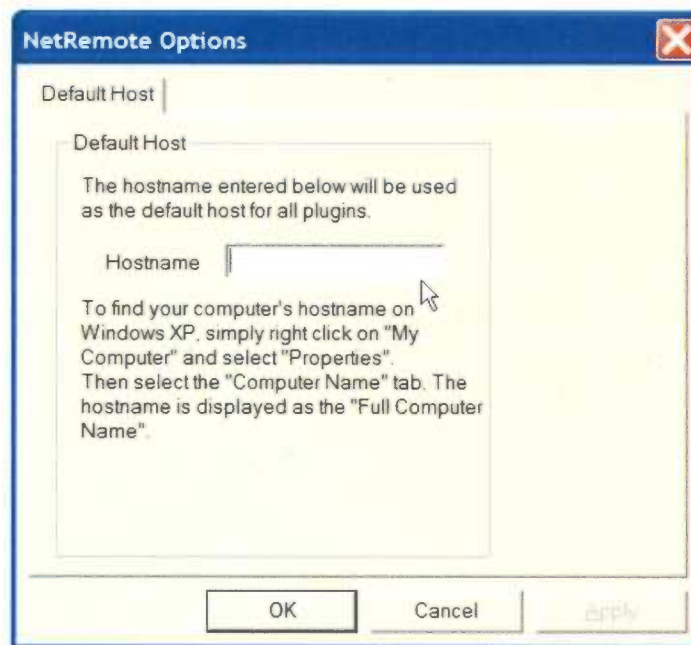


Step 2. Configure NetRemote for Windows.

Start NetRemote. If NetRemote cannot find JRMCM, the screen below will be displayed.



Click OK.



Enter the name or IP address of the computer running JRMCM in to the Hostname box. Click OK. If you do not know the computer name or IP address, follow the steps below.

To find out your PC's Computer Name, press Start and select My Computer. Alternatively, double click the My Computer icon on your desktop.



Click on view system information.

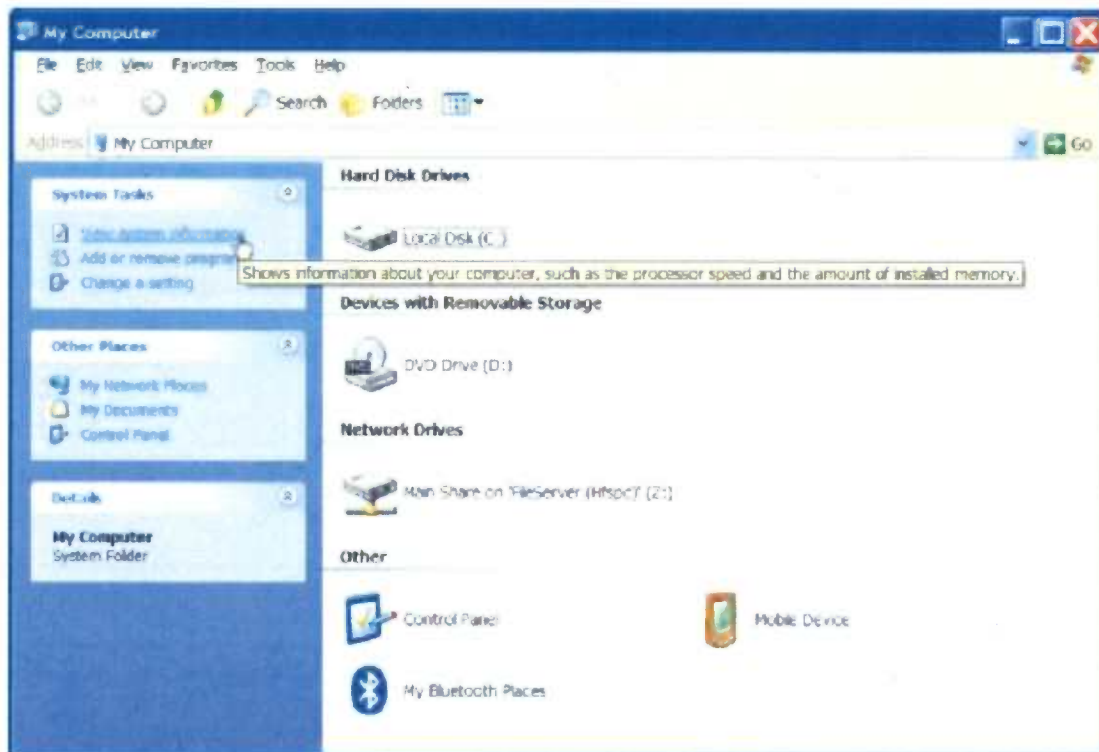
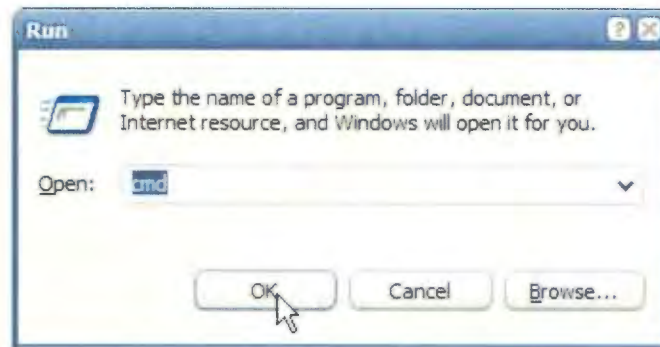


EXHIBIT A

You can also use your computer's IP address. Click the Start button, Run and type in CMD and press Enter as shown below



At the command prompt, type ipconfig and press enter. The computer's IP address is then displayed as shown below.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\TEMP>ipconfig

Windows IP Configuration

Ethernet adapter Home Docking Station:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.1.214
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Builtin Ethernet:

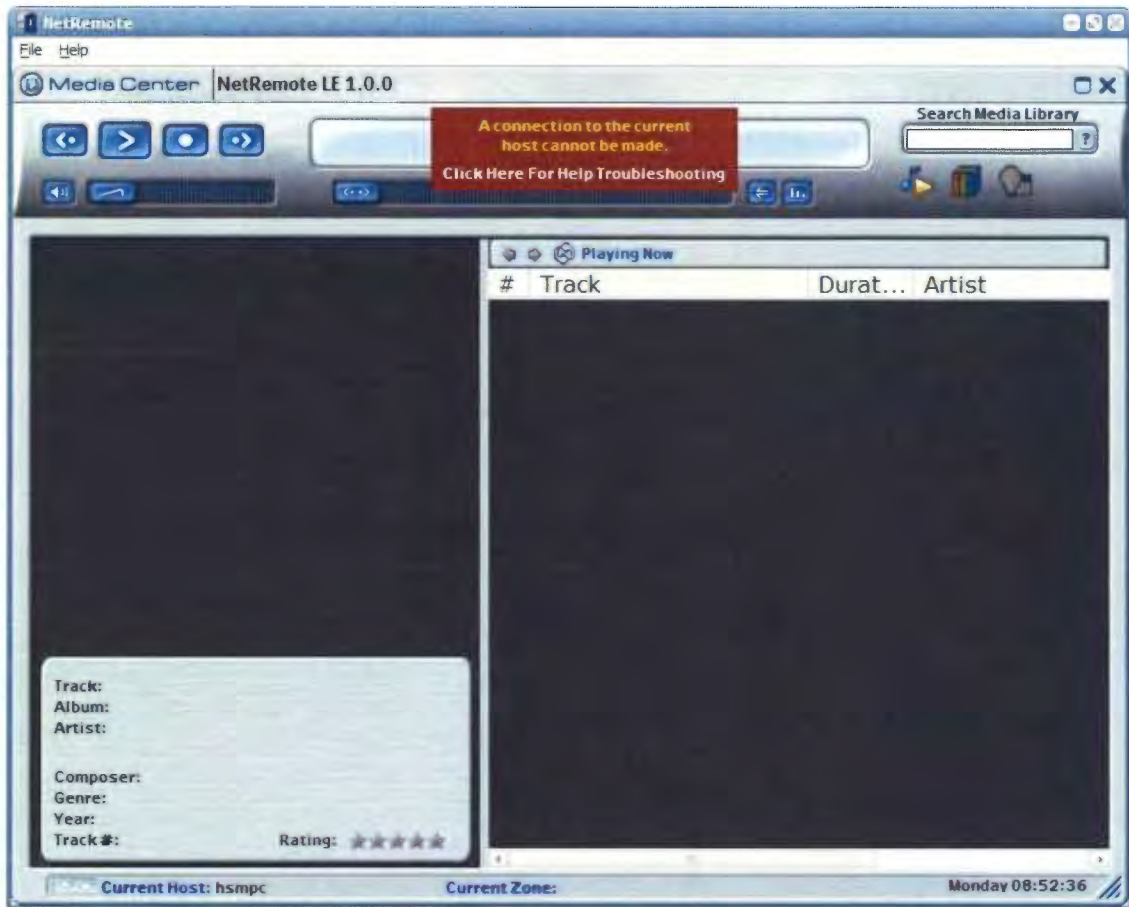
    Media State . . . . . : Media disconnected

C:\Documents and Settings\TEMP>_
```

Type the number in the box (in this case "192.168.1.214"). Type exit to leave the console window.

EXHIBIT A

If NetRemote can still not connect with JRMC, you will see the screen below.

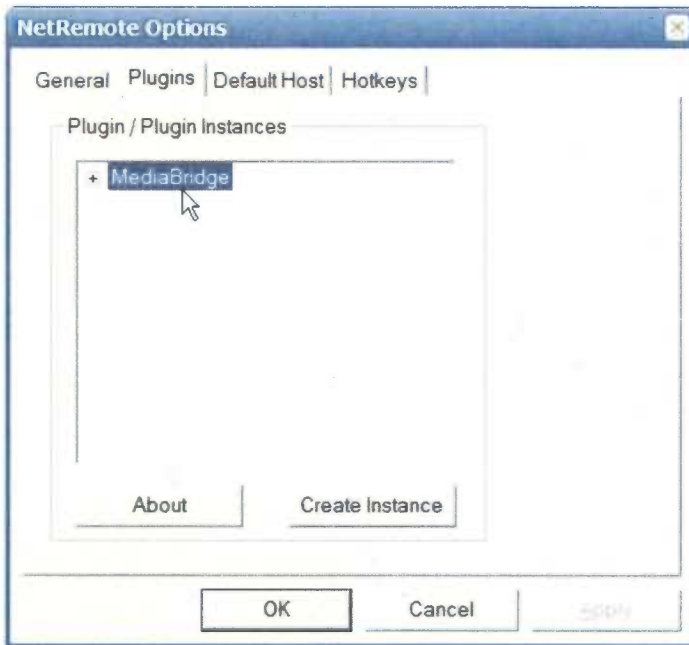


Open the Properties dialog by clicking File/ Properties as shown.

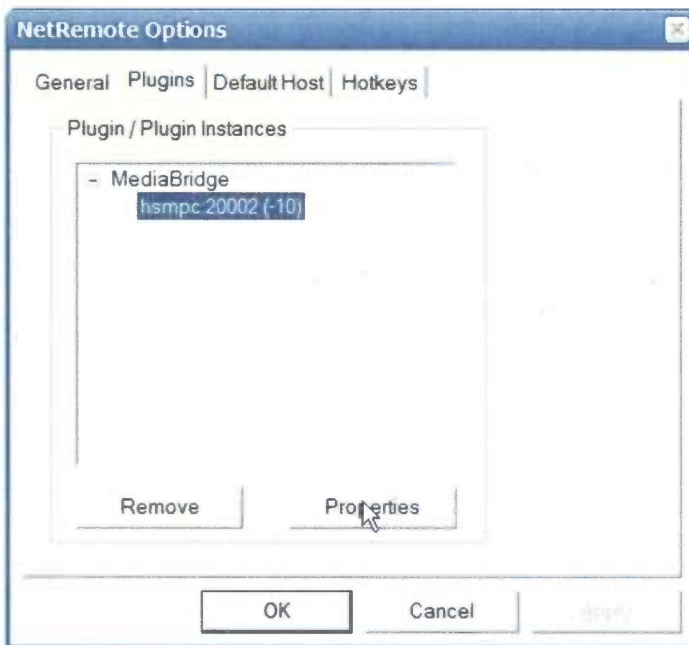


EXHIBIT A

This will display the NetRemote Options dialog. Select the Plugins tab. You should see the screen below.



Double click MediaBridge.



Highlight the first entry and click Properties.

EXHIBIT A

In the Host box, type in the name or IP address of the computer running JRMC. Next enter the same Port number as you used to configure Media Center. Again the default of 20002 should work fine. If you need help finding the IP address of the computer running JRMC, follow the instructions below.

Click OK once you have entered the computer name or IP address.



The JRMC Plugin dialog box contains the following fields and options:

- Host: HSMPC
- Port: 20002
- Default Img Size: XLarge
- Control Font: Verdana
- Library Root: (empty)
- Use "Add To Playlist" Menu
- Show Playing Now In Tree
- Buttons: Cancel, Help, OK



The NetRemote Media Center interface shows the following details:

- Media Center: NetRemote LE 1.0.0
- Current Track: Piano & I (Alicia Keys - Songs In A Minor), 00:07 / 01:51 - 1 of 11
- Search Media Library: MP.SearchString
- Playing Now playlist:

#	Track	Durat...	Artist
1	Piano & I	01:51	Alicia Keys
2	How Come You Don'...	03:50	Alicia Keys
3	A Woman's Worth	05:03	Alicia Keys
4	Jane Doe	03:48	Alicia Keys
5	Goodbye	04:20	Alicia Keys
6	The Life	05:25	Alicia Keys
7	Mr. Man	04:09	Alicia Keys
8	Never Felt This Way...	02:00	Alicia Keys
9	Why Do I Feel So Sad	04:15	Alicia Keys
10	Caged Bird (Outro)	03:02	Alicia Keys
11	Lovin' U	03:48	Alicia Keys

Track details for "Piano & I":

- Track: Piano & I
- Album: Songs In A Minor
- Artist: Alicia Keys
- Composer: Alicia Keys
- Genre: Rock
- Year: 2001
- Track #: 1
- Rating: ★★★★★

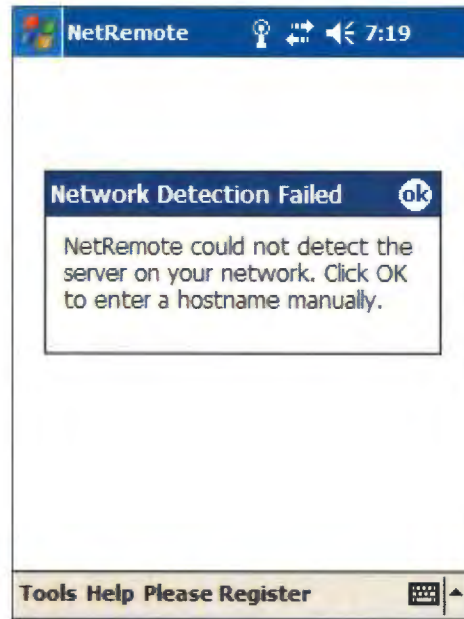
Current Host: olpc | Current Zone: Master Zone | Monday 09:15:09

You will see the screen above when NetRemote connects to JRMC. If you are still experiencing problems, please visit the [NetRemote Forum](#) on the Promixis website

Step 3. Configuring NetRemote for the PPC.

NOTE: This guide assumes your PPC is correctly connected to your network using a wireless connection.

Start NetRemote. If NetRemote cannot find JRMC on your network, the screen below will be displayed.



Tap OK. NetRemote will then ask you to enter the hostname for the computer that you want specified as the default host.

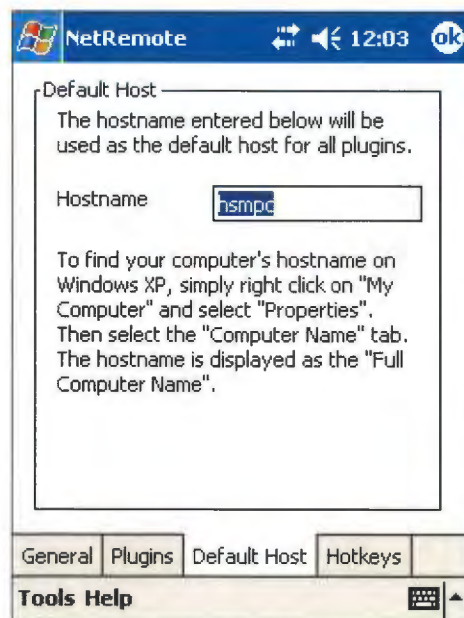


EXHIBIT A

To determine the computer name or IP address using the steps described above for the Windows client.



In the Host box, enter either the computer name or IP address. If you don't know the IP address, see the section above for how to determine it. Next, enter the Port number. The default number, 20002, should be fine unless you changed this when configuring JRMIC.

Tap OK.

If NetRemote is still unable to connect to JRMIC, the screen below will be displayed.

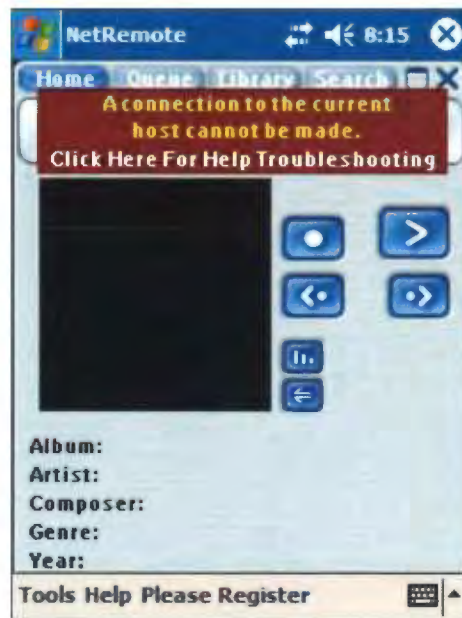
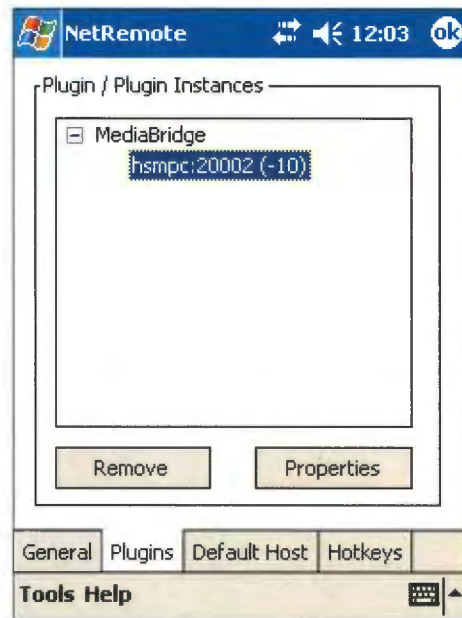
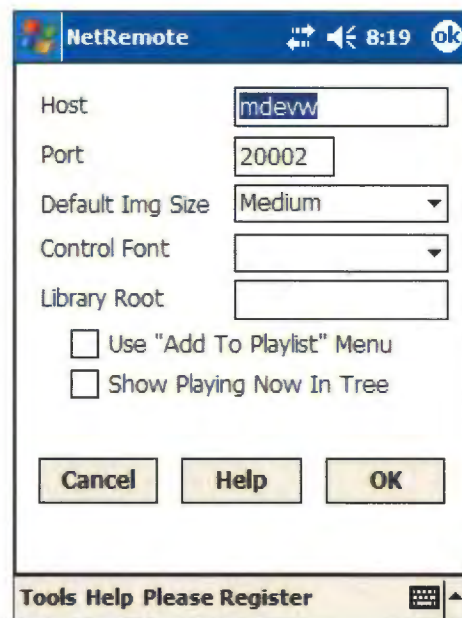


EXHIBIT A

Select Tools/ Properties. Select the Plugins tab. The screen below is displayed.



Click the plus sign next to MediaBridge and highlight the first item. Click Properties.



Make sure the Host name and Port numbers match the entries made when configuring the RemoteServer in JRM. Click OK. If NetRemote still does not connect to JRM, please visit the [NetRemote forum](#) at the [Promixis web site](#).

EXHIBIT A

http://web.archive.org/web/20050120005959/http://promixis.com/pdfs/NetRemote_LE_Installation_Guide.pdf

NetRemote LE Installation Guide for J. River Media Center

1. Download NetRemote.

Download NetRemote LE from [Promixis](#) and save the file on your computer (your Desktop is an easy place). You may delete the installation program when finished.

2. Install NetRemote.

NetRemote is installed by running the file you just downloaded. Double click the file to start the installation process. The first screen is the NetRemote license agreement. Please read this carefully. Each license allows you to install NetRemote on 2 different personal computers (PC's) or pocket PC's (PPC).



Next, you will choose which version of NetRemote to install. If ActiveSync is not detected, only the option for installing the Windows version will be selectable.

3. NetRemote for Windows (98,Me,XP,2000,2003)

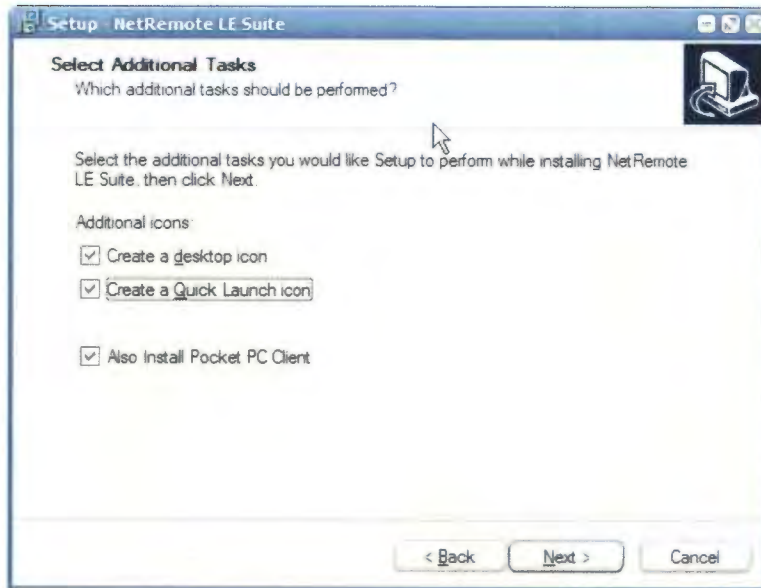
The destination folder is where the NetRemote program is installed on your hard drive. We suggest you use the default folder as shown below. Click **Next** to continue.



Next, select the Start Menu folder. Click **Next** to continue.

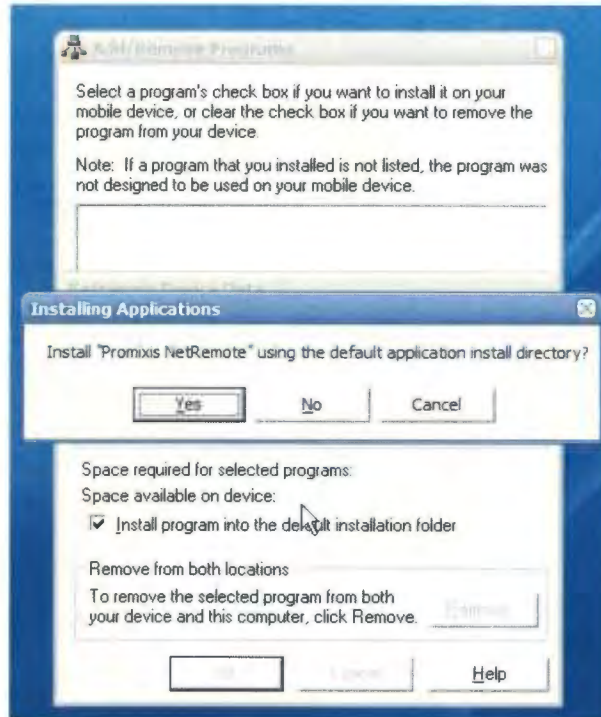


After NetRemote is installed, you can then select to have Short Cuts created on the Desktop and Quick Launch bars. Select the options you want. If you have an ActiveSync connection, the option to install the Pocket PC Client is available. Click **Next** to continue

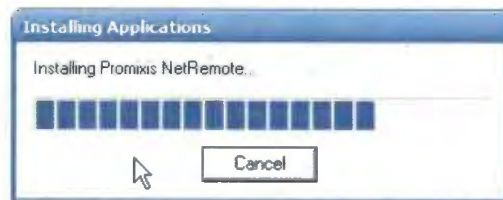


4. NetRemote for the PPC (2002, 2003)

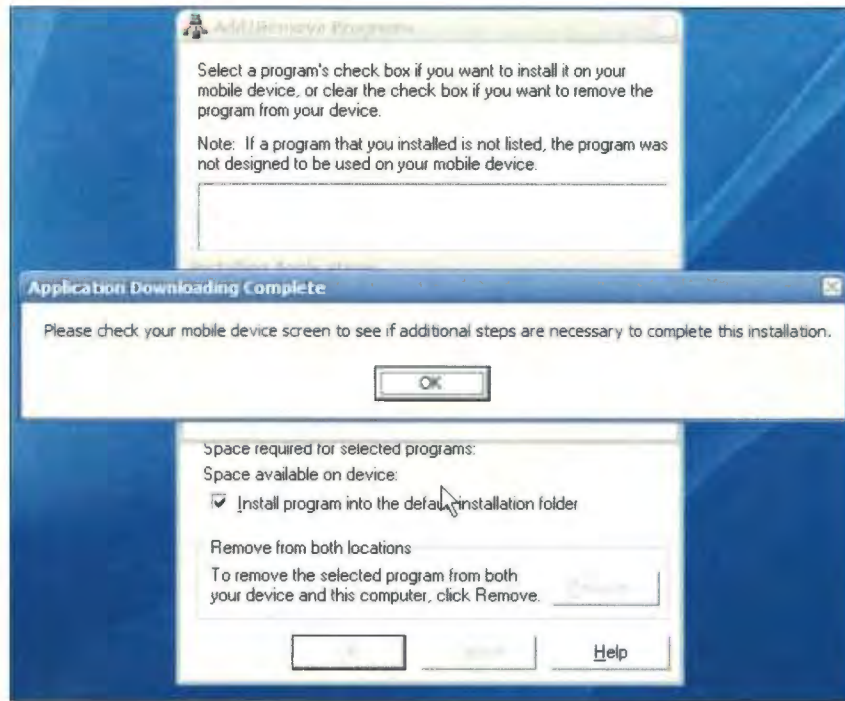
The option for installing the PPC version is only available on computers that have ActiveSync installed. After installing the PPC version, if your PPC is connected, ActiveSync displays the screen below.



Click **Yes** to install in the default directory (suggested). ActiveSync will then display a progress bar as the application is installed.

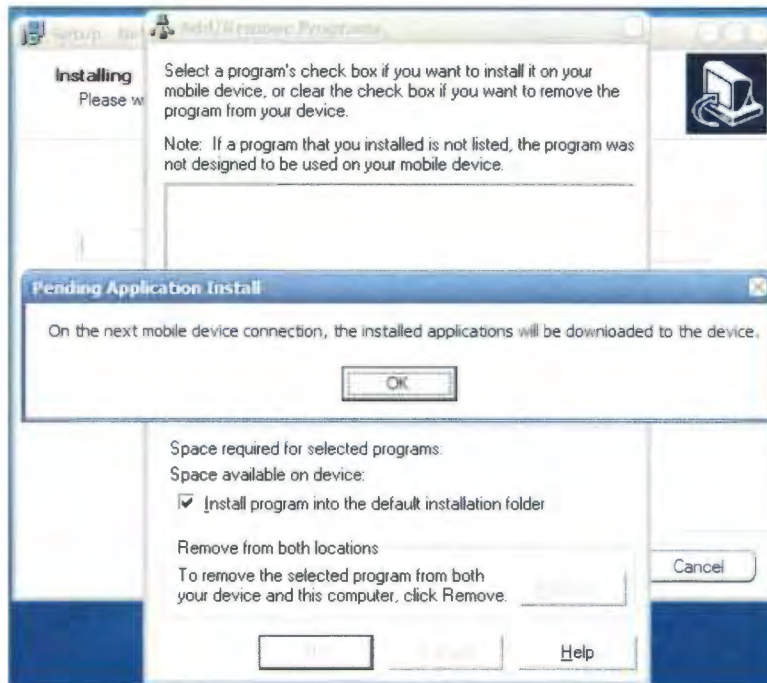


When the installation is completed, ActiveSync will display.



Click **OK** to continue.

If your PPC is not connected to your computer then ActiveSync will show the screen below.



Click **OK** to continue. When you connect your PPC, NetRemote will be installed as described above. See your PPC device and follow the instructions on the screen.



5. Final Steps

Before the installation ends, you will have the option to start Media Center (if installed on this PC) and to launch NetRemote (if installed on this PC). It is recommended you start Media Center prior to starting NetRemote so that NetRemote can automatically configure the network settings for you.

Please see the **NetRemote LE Network Configuration Guide** for setting up NetRemote on your network.

EXHIBIT A

http://web.archive.org/web/20050119225451/http://promixis.com/pdfs/NetRemote_LE_Setup_Guide.pdf

NetRemote LE Setup Guide

This guide explains how to setup the NetRemote MediaBridge plugin for J. River's Media Center. For problems with network configuration, please see the NetRemote LE Network Configuration Guide.

Start either the NetRemote Windows or Pocket PC client.

Open the Properties Page.

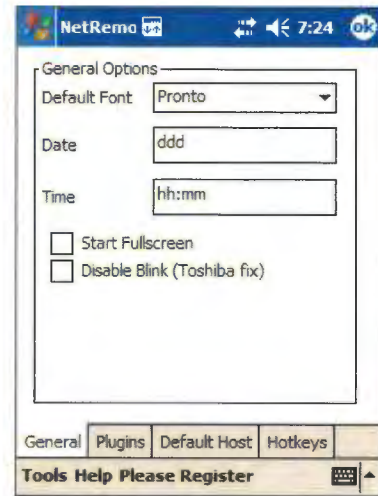
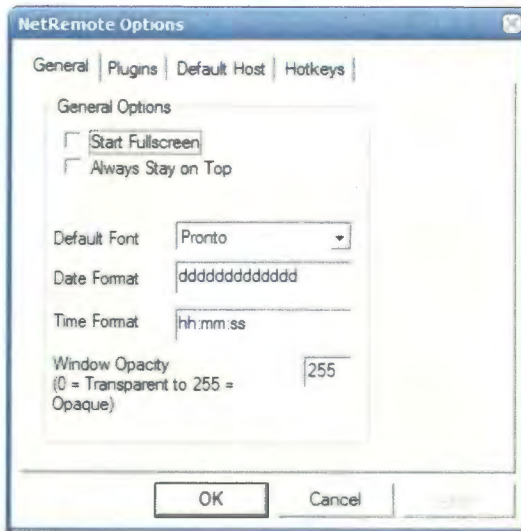
For the Windows client, click File/ Properties.



For the Pocket PC client, tap Tools/ Properties.



General Tab



Start Full Screen sets NetRemote to start up full screen.

Always On Top Option (Windows Client Only) keeps NetRemote always visible.

Default Font sets the font used to draw buttons and labels. In most instances, this should not be changed.

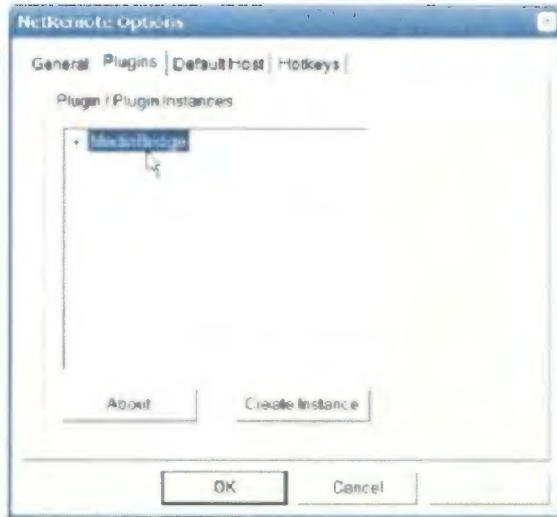
Date Format controls how the day of the week is displayed. Each "d" represents one letter, ie. "ddd" for Monday will show "Mon".

Time Format controls how the time is displayed. "hh:mm:ss" will show the hour, minute, second.

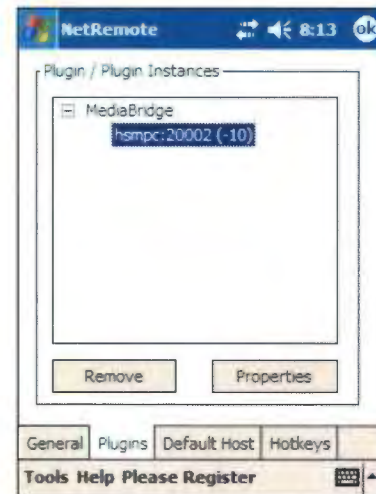
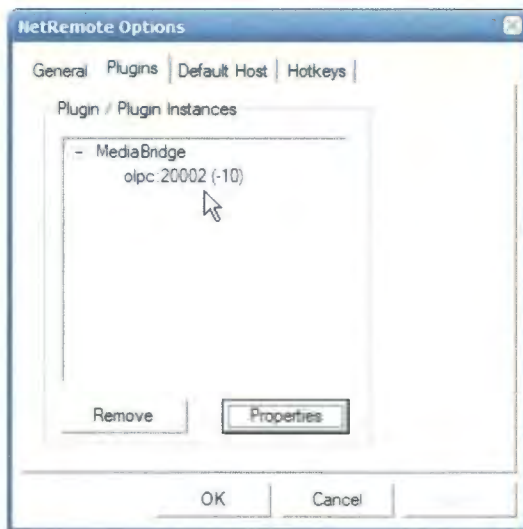
Window Opacity (Windows Client Only) is used to make the NetRemote window transparent. Values less than 200 are not recommended. This setting is useful with the Always On Top option.

Plugins Tab

On this tab, the list of NetRemote plugins are displayed. In the LE or IR editions of NetRemote, this is limited to the MediaBridge and IR plugins respectively.



Each plugin can have multiple “instances”. This allows NetRemote to communicate with more than one server. For instance, you could have Media Center running on multiple computers. Click on the plus sign to view a list of connections. The screen will change as shown below.



To change the configuration of an instance of the plugin, click on it to highlight it and then click on Properties. This will bring up the next dialog box.

MediaBridge Properties

JRMPC Plugin

Host: HSMPC

Port: 20002

Default Img Size: XLarge

Control Font: Verdana

Library Root:

Use "Add To Playlist" Menu

Show Playing Now In Tree

Cancel Help OK

NetRemo

Host:

Port: 20002

Default Img Size: Medium

Control Font:

Library Root:

Use "Add To Playlist" Menu

Show Playing Now In Tree

Cancel Help OK

Tools Help Please Register

Host specifies the computer that this instance of the plugin connects to. This can be the computer name or the IP address.

Port specifies the port that NetRemote uses.

Default Img Size is the size of cover art images that NetRemote will use. On windows clients use Large or XLarge. On Pocket PC devices, you may want to use Medium or smaller. This is done for performance reasons.

Control Font specifies the font used to display the media library and playing now lists.

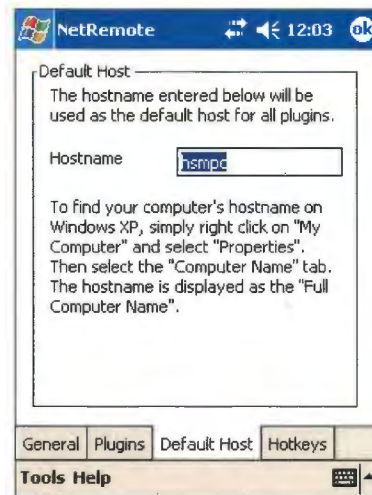
Library Root is used with Media Center. It specifies where in the Media Library that NetRemote should begin displaying from.

Use "Add to Playlist" Menu adds the option to add songs to a playlist in Media Center. This option may cause performance problems on slower Pocket PC clients.

Show Playing Now in Tree will display the currently playing songs in the Media Library tree.

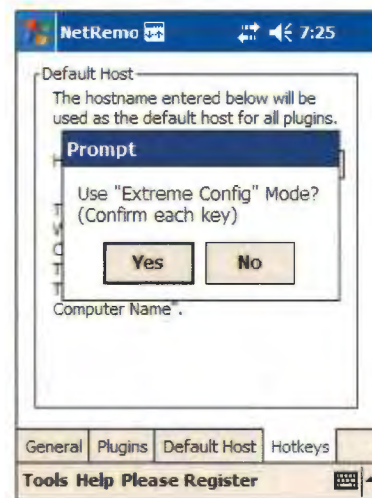
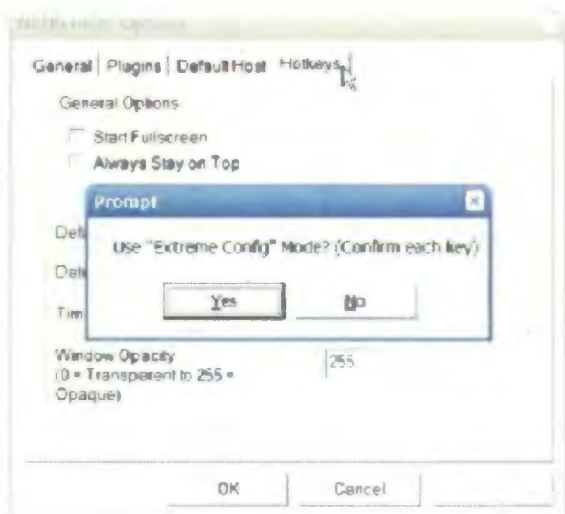
Press OK to save you changes.

Default Host Tab



Default Host specifies with host computer NetRemote should connect with first. Enter either the computer name or IP address in this box. Click OK when done.

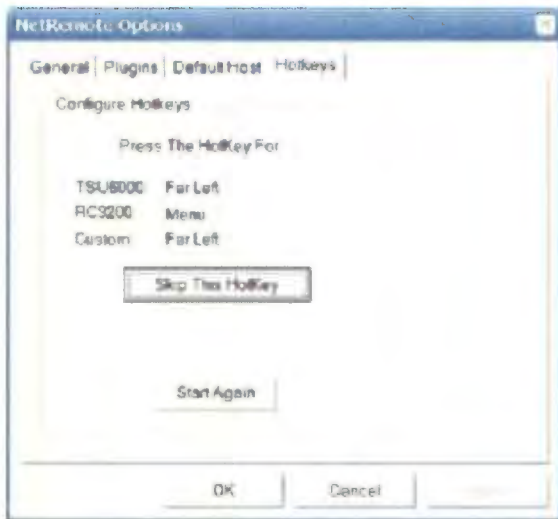
HotKeys Tab



The Extreme Config mode is usually not necessary. Click NO unless you are having problems configuring your device.

EXHIBIT A

NetRemote will then configure all of the HotKeys found on the Pronto (or similar) remote controls. The commands these keys are linked to are specified in the current CCF file.



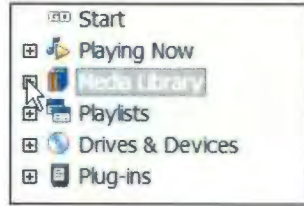
Configuring J. River Media Center for Album Covers View

NetRemote will display all of your albums by cover art, as shown below. This requires you to create a new View Scheme in JRMC.



Adding the album cover art View Scheme to JRMCM:

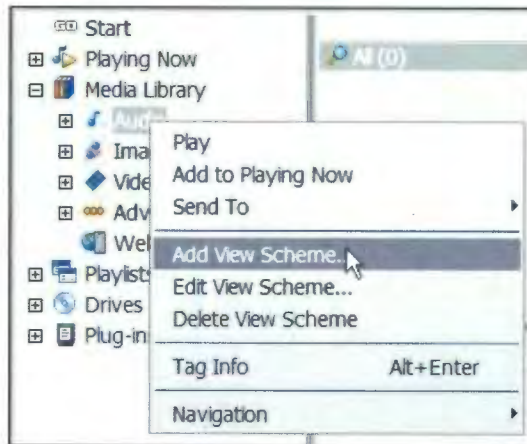
1. Start JRMCM.
2. Open up the Media Library tree by clicking on the plus sign.



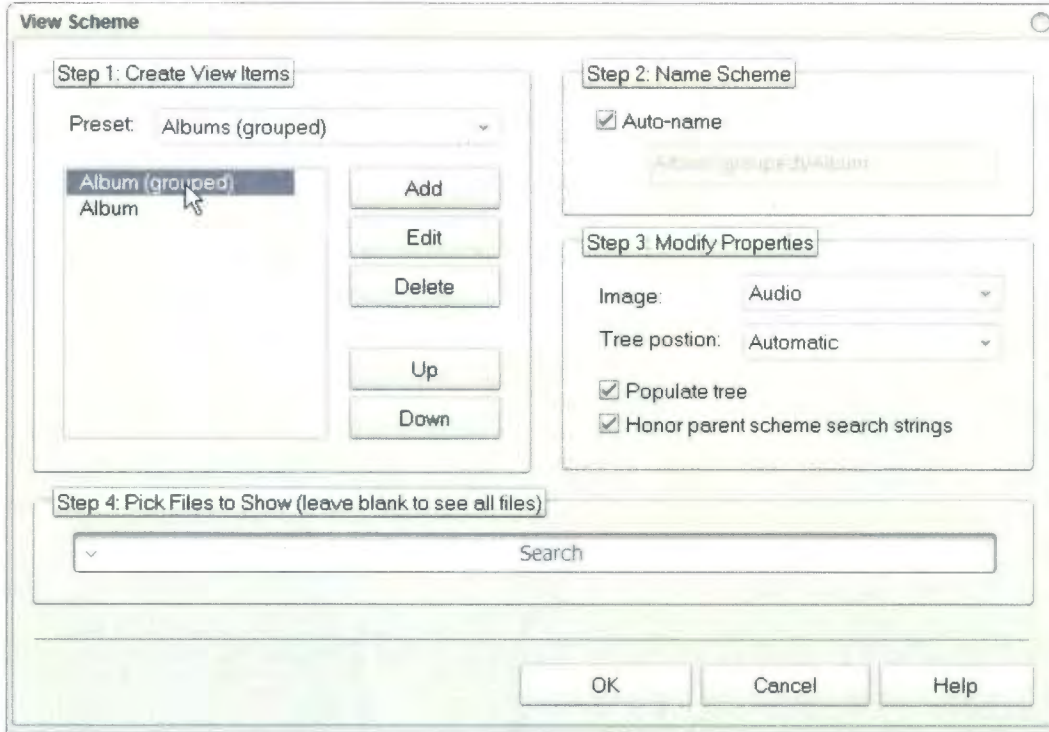
3. Right Click Audio.



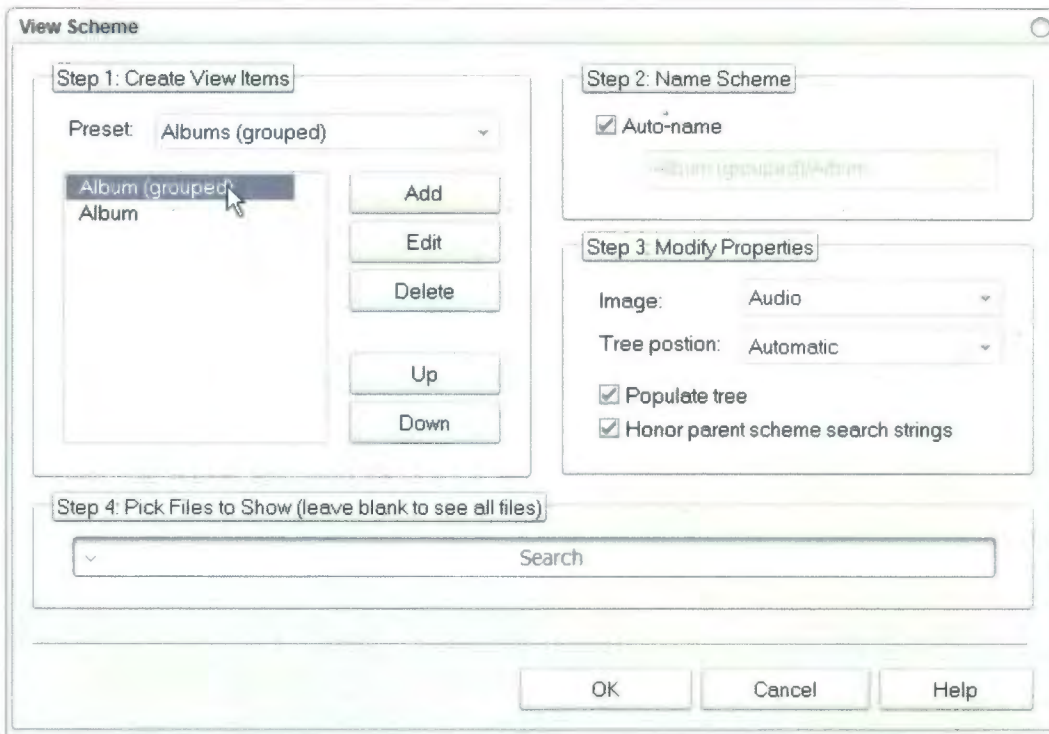
4. Click Add View Scheme.



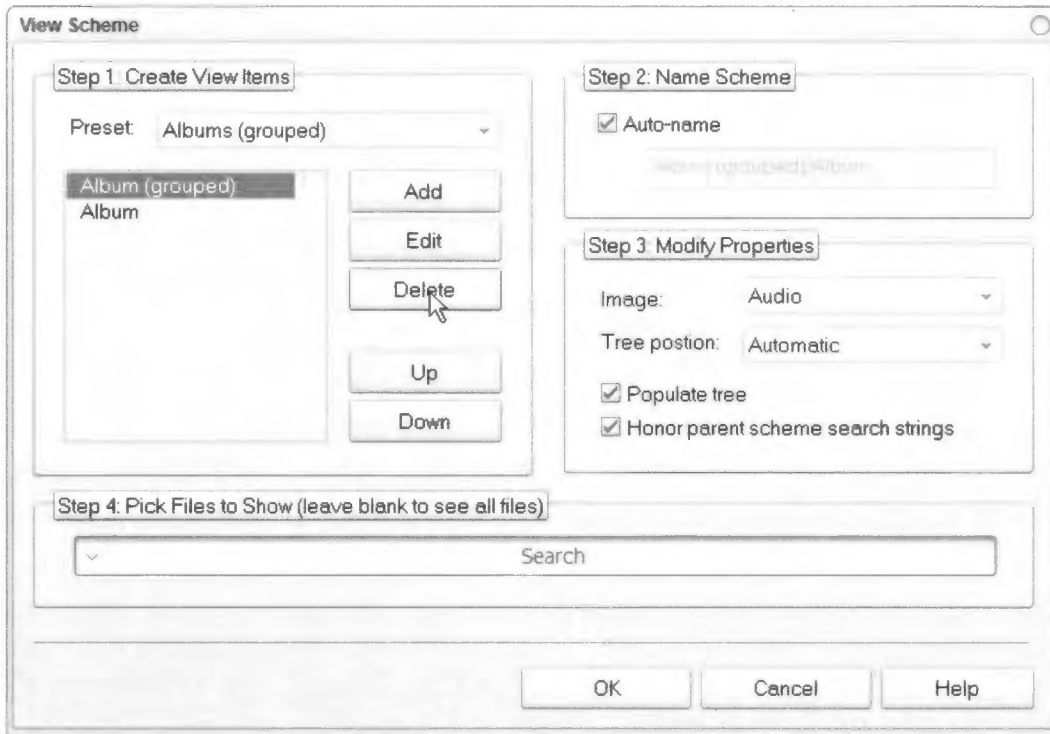
5. Select Album (Grouped).



6. Select the Album (Grouped) text.



7. Click Delete.



8. Click OK.

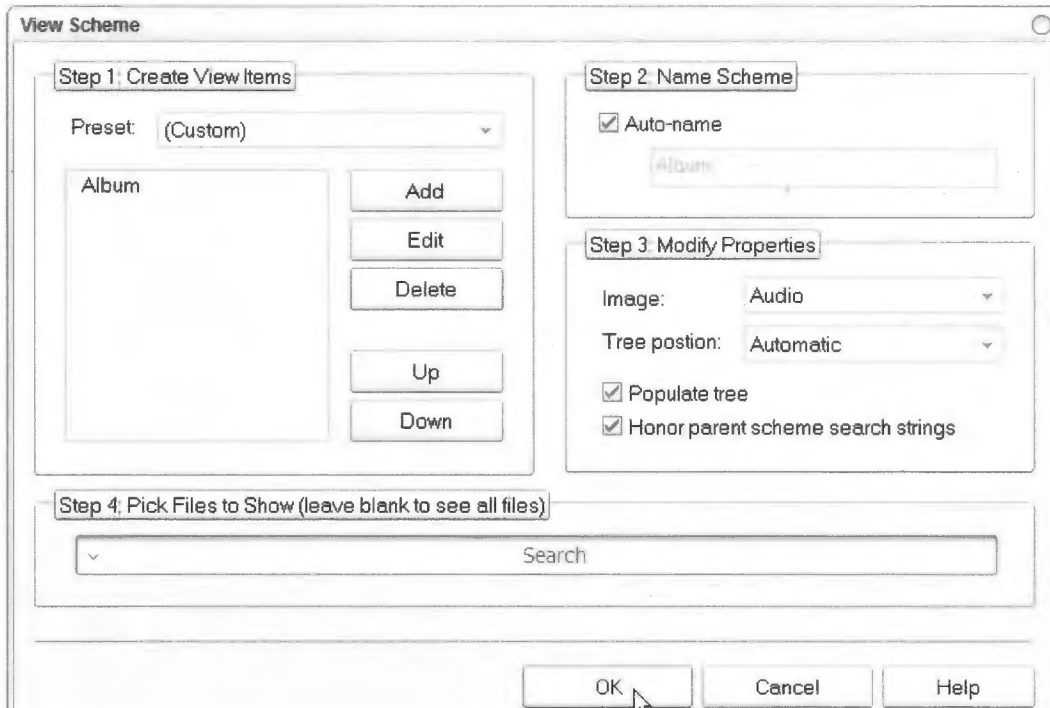


EXHIBIT A

http://web.archive.org/web/20050119225826/http://promixis.com/pdfs/NetRemote_LE_Network_Configuration_Guide.pdf

NetRemote LE Network Configuration Guide

Automatic Network Configuration

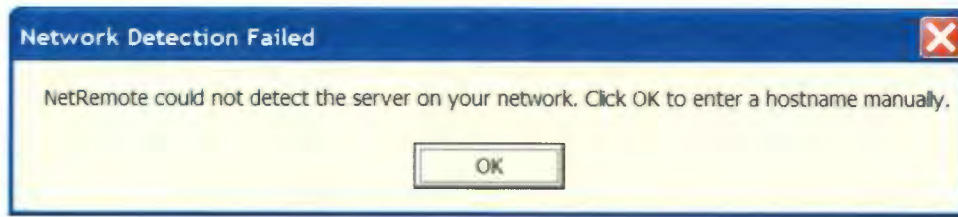
NetRemote works by “talking” to J. River Media Center (JRMC) over your network. It works with both wired and wireless networks. NetRemote is designed to automatically configure and connect to any computers on your network running JRMC. You must have your devices already connected to your network before configuring NetRemote.

Start J. River Media Center on your computer.

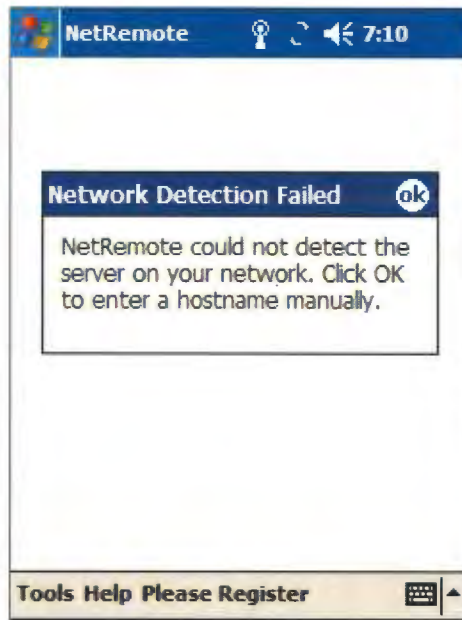
Start NetRemote (either the Windows or Pocket PC version). NetRemote will take a few seconds to examine your network and try and find any computer that is running JRMC. After NetRemote has completed this step, you will see a screen similar to below, depending on what Media Center is playing.



If NetRemote cannot connect to JRMC you will see this message on the Windows Client.



On the Pocket PC client you will see this message.



Proceed to the Manual Configuration guide below.

Manual Network Configuration

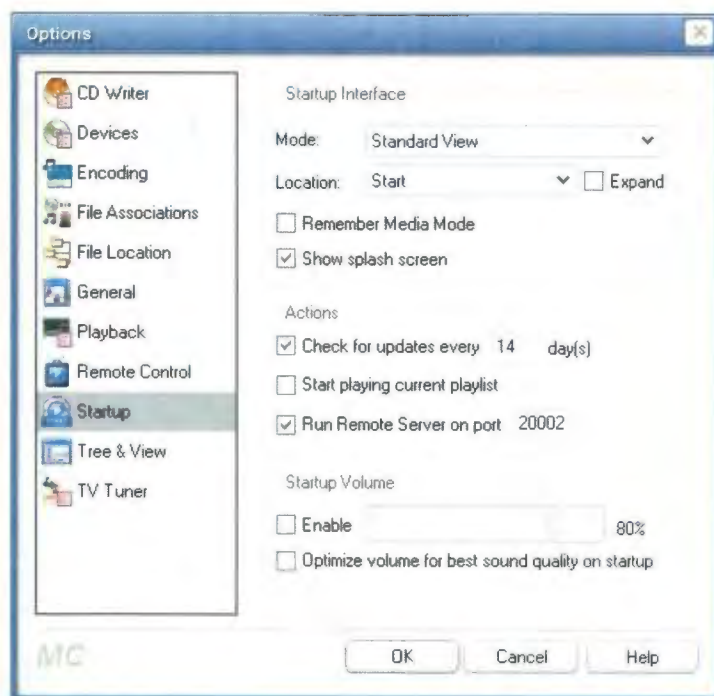
In some instances, depending on your network configuration and security settings, automatic configuration may not work. In this case, follow the steps below.

Step 1. Configure J. River Media Center (JRMC)

Start JRMC. Open up the Options dialog by pressing Ctrl-O or from the Tools Menu.



The Options dialog is then displayed. Select Startup. Under actions, check the Run Remote Server box and specify the port address. In most installations the default port of 20002 will work fine. Click OK. You are now finished setting up JRMC. Leave JRMC running.

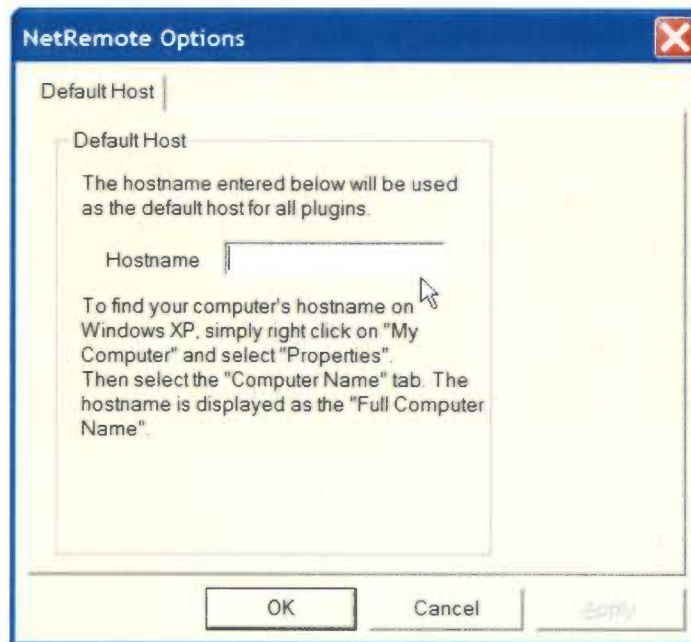


Step 2. Configure NetRemote for Windows.

Start NetRemote. If NetRemote cannot find JRMCI, the screen below will be displayed.

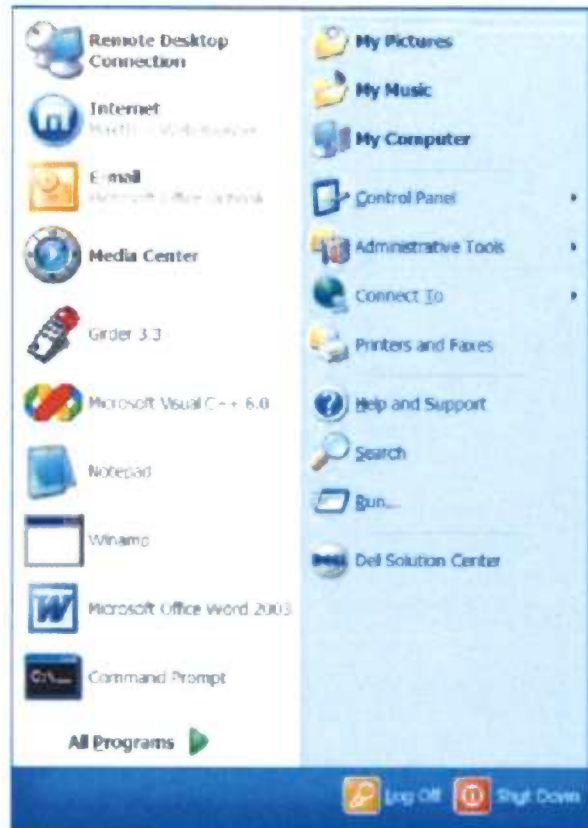


Click OK.



Enter the name or IP address of the computer running JRMCI into the Hostname box. Click OK. If you do not know the computer name or IP address, follow the steps below.

To find out your PC's Computer Name, press Start and select My Computer. Alternatively, double click the My Computer icon on your desktop.



Click on view system information.

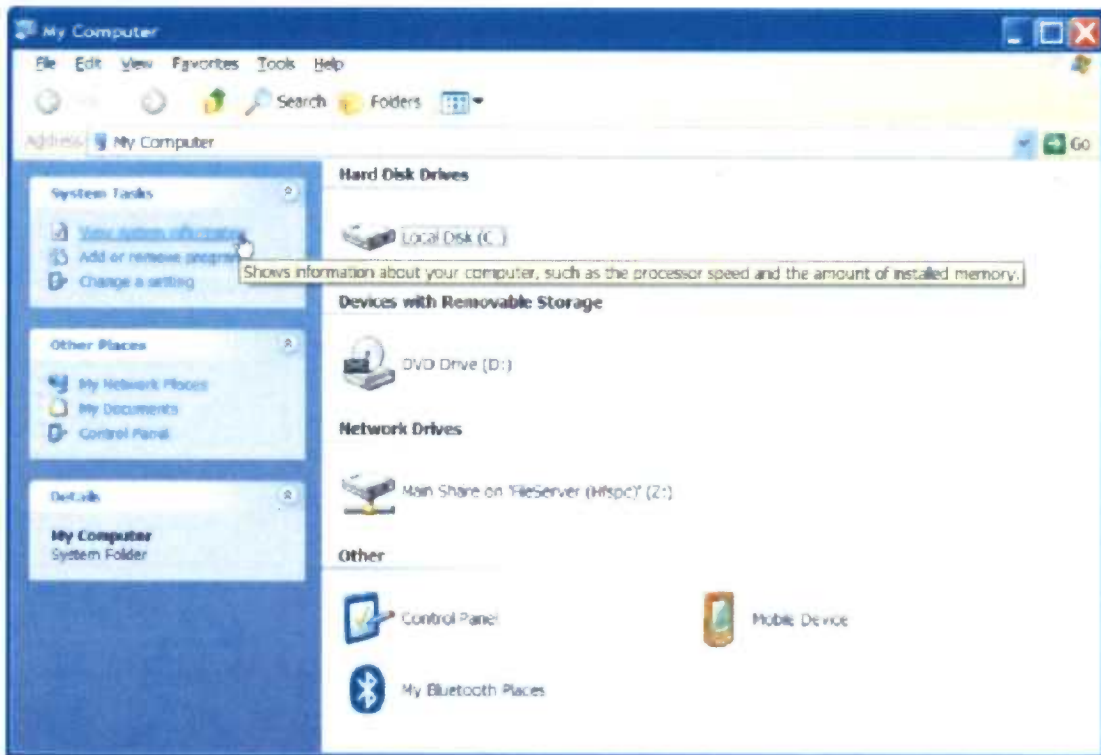
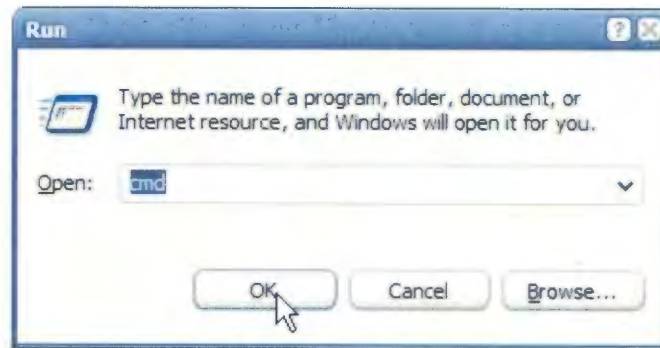
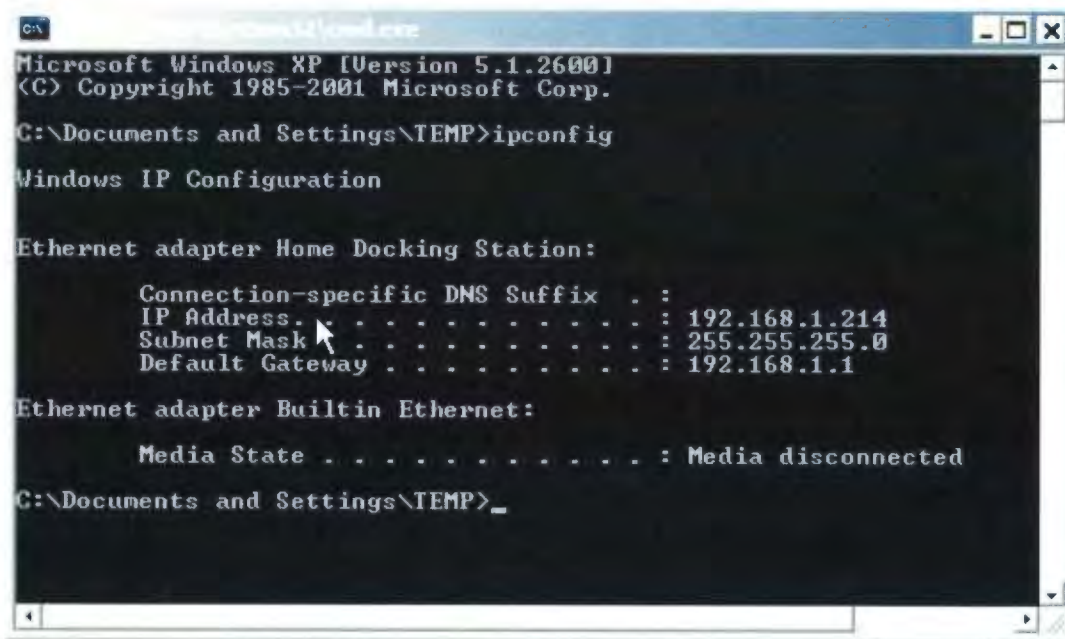


EXHIBIT A

You can also use your computer's IP address. Click the Start button, Run and type in CMD and press Enter as shown below



At the command prompt, type ipconfig and press enter. The computer's IP address is then displayed as shown below.

A screenshot of a Windows command prompt window. The title bar shows 'C:\>cmd.exe'. The window content shows the following text:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\TEMP>ipconfig

Windows IP Configuration

Ethernet adapter Home Docking Station:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.214
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

Ethernet adapter Builtin Ethernet:

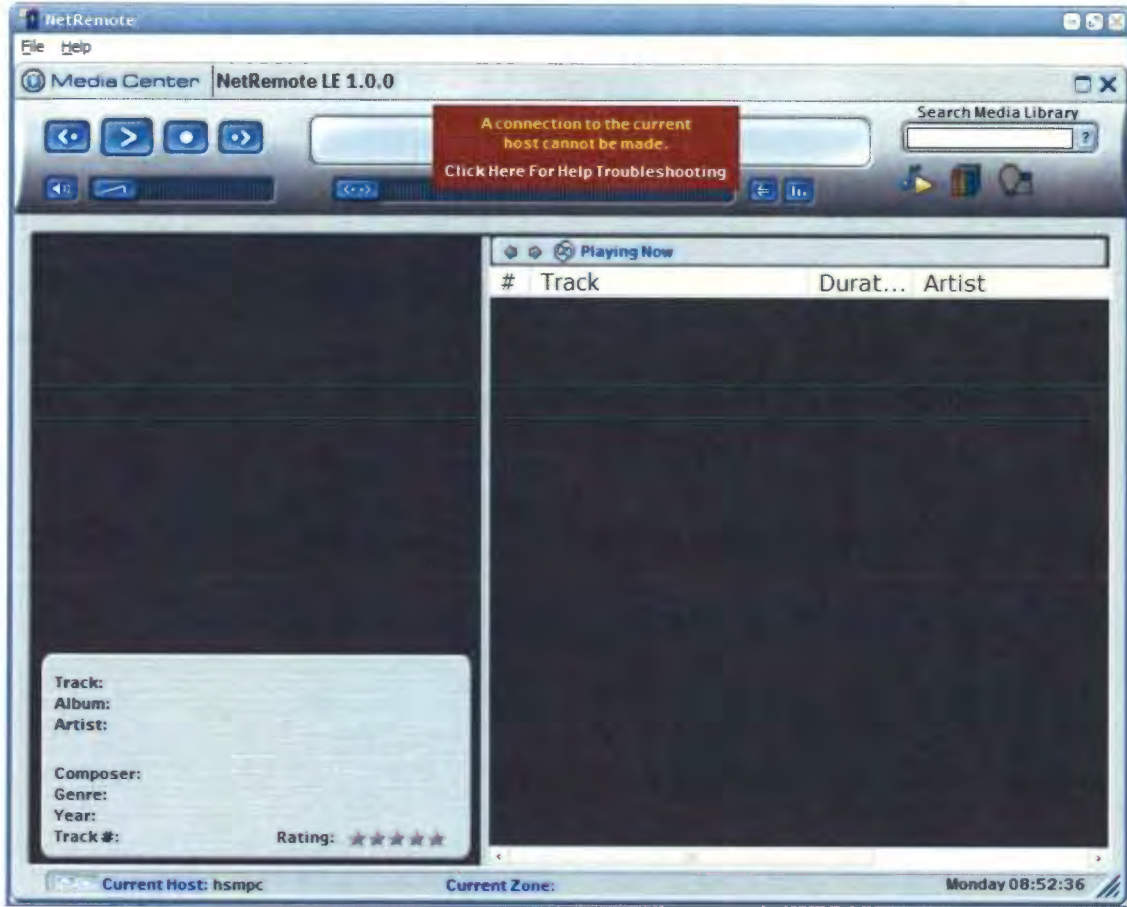
    Media State . . . . .             : Media disconnected

C:\Documents and Settings\TEMP>_
```

Type the number in the box (in this case "192.168.1.214"). Type exit to leave the console window.

EXHIBIT A

If NetRemote can still not connect with JRMC, you will see the screen below.

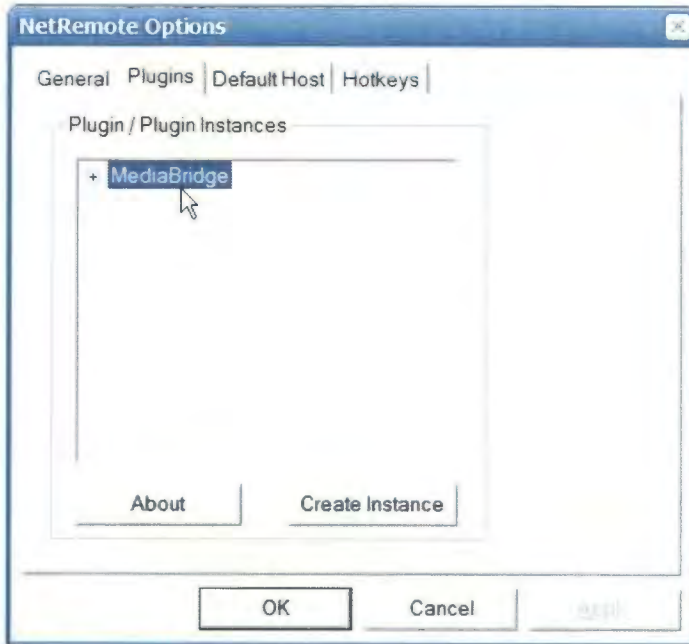


Open the Properties dialog by clicking File/ Properties as shown.

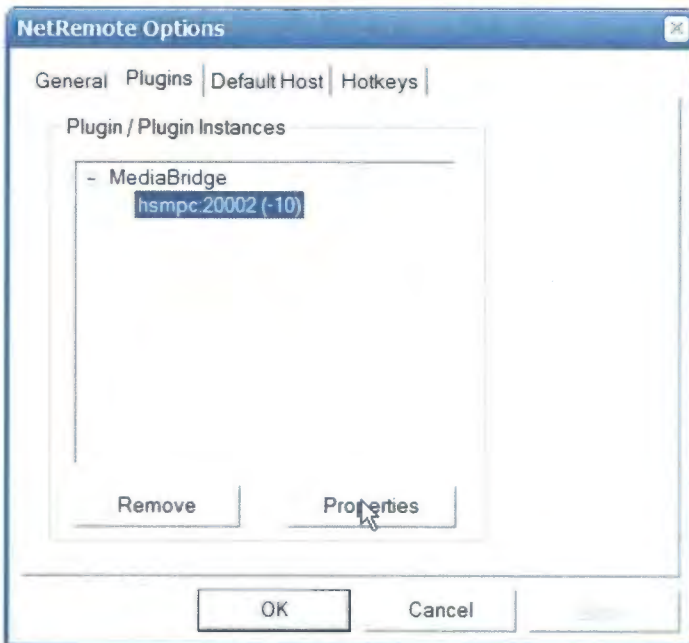


EXHIBIT A

This will display the NetRemote Options dialog. Select the Plugins tab. You should see the screen below.



Double click MediaBridge.



Highlight the first entry and click Properties.

EXHIBIT A

In the Host box, type in the name or IP address of the computer running JRMC. Next enter the same Port number as you used to configure Media Center. Again the default of 20002 should work fine. If you need help finding the IP address of the computer running JRMC, follow the instructions below.

Click OK once you have entered the computer name or IP address.



The JRMC Plugin dialog box contains the following fields and options:

- Host: HSMPC
- Port: 20002
- Default Img Size: XLarge
- Control Font: Verdana
- Library Root: (empty)
- Use "Add To Playlist" Menu
- Show Playing Now In Tree
- Buttons: Cancel, Help, OK



The NetRemote LE 1.0.0 interface shows the following details:

- Media Center: NetRemote LE 1.0.0
- Playing Now: Piano & I (Alicia Keys - Songs In A Minor) 00:07 / 01:51 - 1 of 11
- Search Media Library: MP.SearchString ?
- Track List:

#	Track	Durat...	Artist
1	Piano & I	01:51	Alicia Keys
2	How Come You Don'...	03:50	Alicia Keys
3	A Woman's Worth	05:03	Alicia Keys
4	Jane Doe	03:48	Alicia Keys
5	Goodbye	04:20	Alicia Keys
6	The Life	05:25	Alicia Keys
7	Mr. Man	04:09	Alicia Keys
8	Never Felt This Way...	02:00	Alicia Keys
9	Why Do I Feel So Sad	04:15	Alicia Keys
10	Caged Bird (Outro)	03:02	Alicia Keys
11	Lovin' U	03:48	Alicia Keys

Track details for "Piano & I":

- Track: Piano & I
- Album: Songs In A Minor
- Artist: Alicia Keys
- Composer: Alicia Keys
- Genre: Rock
- Year: 2001
- Track #: 1
- Rating: ★★★★★

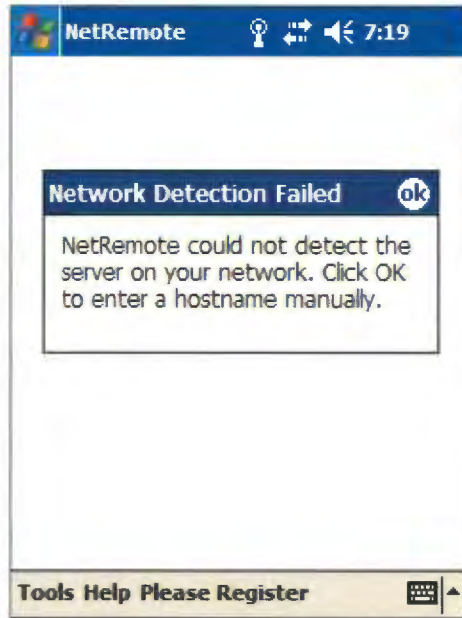
Current Host: olpc | Current Zone: Master Zone | Monday 09:15:09

You will see the screen above when NetRemote connects to JRMC. If you are still experiencing problems, please visit the [NetRemote Forum](#) on the Promixis website

Step 3. Configuring NetRemote for the PPC.

NOTE: This guide assumes your PPC is correctly connected to your network using a wireless connection.

Start NetRemote. If NetRemote cannot find JRMCM on your network, the screen below will be displayed.



Tap OK. NetRemote will then ask you to enter the hostname for the computer that you want specified as the default host.

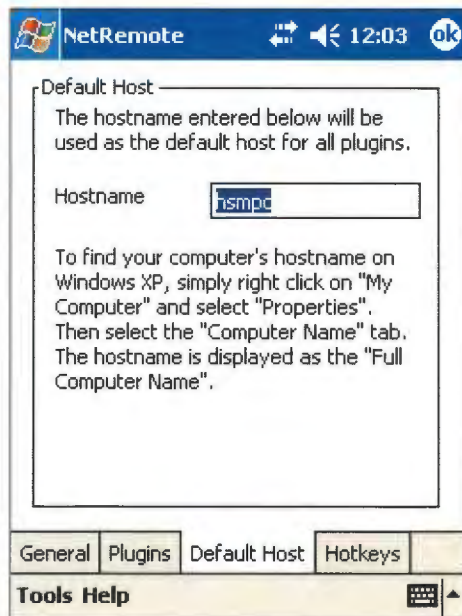
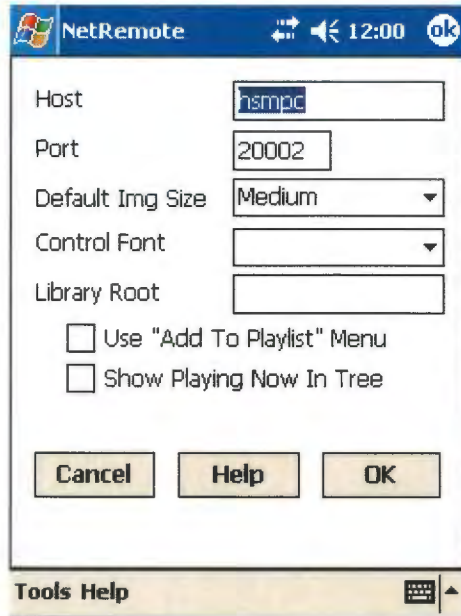


EXHIBIT A

To determine the computer name or IP address using the steps described above for the Windows client.



In the Host box, enter either the computer name or IP address. If you don't know the IP address, see the section above for how to determine it. Next, enter the Port number. The default number, 20002, should be fine unless you changed this when configuring JRMC.

Tap OK.

If NetRemote is still unable to connect to JRMC, the screen below will be displayed.

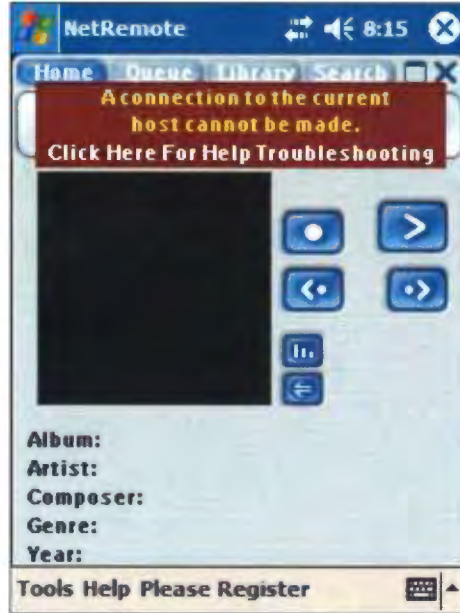
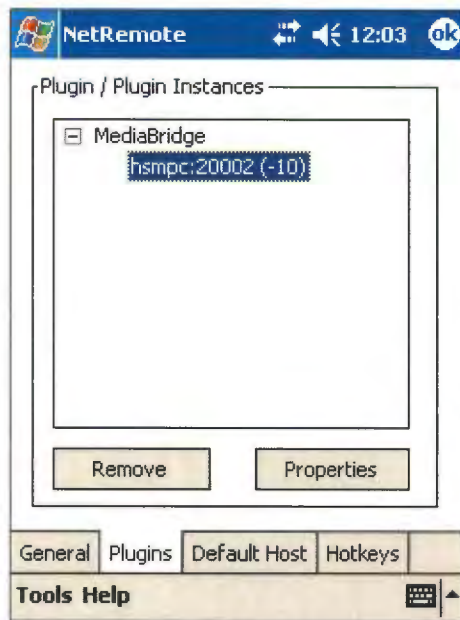
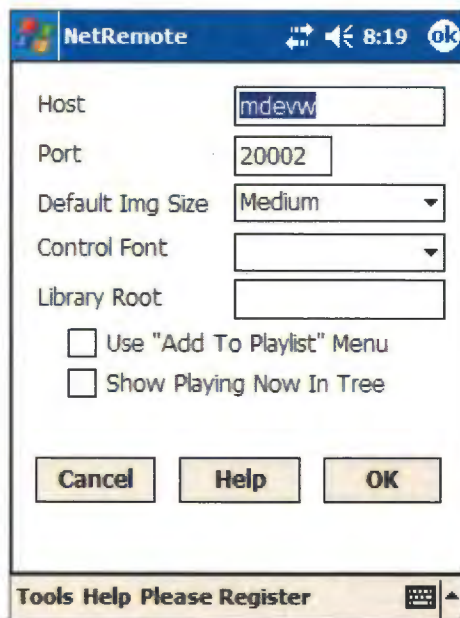


EXHIBIT A

Select Tools/ Properties. Select the Plugins tab. The screen below is displayed.



Click the plus sign next to MediaBridge and highlight the first item. Click Properties.



Make sure the Host name and Port numbers match the entries made when configuring the RemoteServer in JRM. Click OK. If NetRemote still does not connect to JRM, please visit the [NetRemote forum](#) at the [Promixis web site](#).



pdabuyersguide
PDA, Smartphone, Tablet and Ultralight
Notebook Reviews

Palm
Clie
Pocket PC
Linux
Smartphone
Notebook
Accessories
Software
Discuss

- PDA Reviews
- Palm
- Pocket PC
- Sony Clie
- Linux PDAs
- Smartphone
- Handheld PCs & .NET
- Psion
- Tablets & Notebooks
- Discussion Forum
- Accessory Reviews
- Cases
- Keyboards
- GPS
- WiFi Cards
- Bluetooth
- Storage Cards
- Presentation Cards
- Cameras
- iPAQ Sleeves
- Interviews
- Software Reviews
- Sitemap
- About Us
- Contact Us
- Search
- Our PalmGear Store

News of Note:

HP Issues ROM Update for iPAQ 3715
Review: Averatec C3500 Windows XP Tablet Notebook
Sony U Series Comes to America
Treo 650 Pre-order Opens on Sprint Network
Review: Motorola MPx220 MS Smartphone
Pocket PC Game Podz Reviewed and Give-away
[...More News](#)

Motorola MPx220: The new MS Smartphone on the block packs an amazing number of features into a small package. This trim clamshell phone runs MS Smartphone 2003 SE, has a fast processor, Bluetooth, a 1MP camera, an expansion slot and MP3 stereo playback. It's a GSM world phone offered by Cingular in the US.
[Read the review.](#)

palmOne Tungsten T5: The T5 is palmOne's new flagship model, offering a high res + 320 x 480 color display, slate design, Bluetooth, a 416MHz processor and a whopping 256 megs of RAM that will survive a hard reset or complete battery drain. It runs Palm OS 5.4.5 and features a new USB drive mode that allows you to view the PDA's contents as if it were a removable USB drive. Pretty cool!
[Read the review.](#)

Averatec C3500 Tablet: Averatec makes the most affordable Windows XP Tablet on the market. This convertible design notebook doubles as a standard notebook and a tablet. It has a mobile Althon processor, 512 megs of RAM and an integrated DVD+CD-RW optical drive. And of course there's WiFi, Ethernet and more on this 5.5 lb. unit.
[Read the review.](#)

HP iPAQ hx4705: This has been the month of the iPAQ with so many new models released! The hx4705 is one of the most anticipated because it features a fantastic VGA display and a super-fast 624MHz processor. Heap on plenty of memory, Bluetooth, WiFi, both CF and SD slots and a touch pad navigator and you've got the 4705. It's one of only two Pocket PCs with a VGA display sold in the US.
[Read the review.](#)

Dell Axim X50v: Dell's first VGA Pocket PC is a winner. This guy crams a lot in for \$499, offering a 624MHz XScale processor, Intel 2700G accelerated 3D graphics, plenty of memory, Bluetooth, WiFi and dual expansion slots. A fast unit with a pleasing VGA display that should be a hit.
[Read the review.](#)

HP iPAQ rx3715: This is HP's top-of-the-line rx3000 series model, which focuses on multimedia features and good performance. The rx3715 has an excellent 1.2MP camera, a 400MHz processor, lots of memory and runs Windows Mobile 2003 SE. If that's not enough, it has Bluetooth, WiFi, and Nevo AV remote software.
[Read the review.](#)

palmOne Zire 72: This update to the hugely popular Zire 71 offers several significant improvements. The Zire 72 is the first PDA to use the new Intel Bulverde PXA270 processor running at 312 MHz. It has a 1.2 MP camera, an MP3 player, Bluetooth and a great software bundle.
[Read the review.](#)

Samsung i700 Pocket PC Phone: This 2nd generation Pocket PC phone runs on the Verizon Wireless network in the US. It's got a lovely transfective display, a 300 MHz XScale processor, 64 megs of RAM, a VGA camera and an SD slot that supports SDIO. That's a lot of features, and it has great voice quality too! It comes with Pocket PC 2002 Phone Edition OS and supports Verizon's high speed 1xRTT Express Network for data speeds averaging 60 - 70 Kbps.
[Read more.](#)

palmOne Zire 31: Meet the least expensive color PDA on the market. This \$149 model packs a lot of features into a compact and affordable package. It has a 200 MHz processor, color display, SD expansion slot and an MP3 player.
[Read the review.](#)

ASUS A730: Very, very nice! A reasonably priced VGA Pocket PC that's attractive and compact. It has a 520MHz processor running on Windows Mobile 2003 SE, a 1.3MP digicam, Bluetooth and both CF and SD slots. That VGA screen is very sharp and colorful: definitely a model to consider.
[Read the review.](#)

XML New Accessory & Software Reviews

palmOne SD Wi-Fi Card
Finally, an SD WiFi Card for the Tungsten T3 and Zire 72. This excellent card works well and includes a VPN client. 

Logitech Mobile Freedom Bluetooth Headset
This 2nd generation headset is extremely light, attractive and ergonomic. It features "WindStop" technology to reduce outgoing background noise levels. 

IOGEAR USB Bluetooth Adapter
This Bluetooth adapter works with PCs and Macs, and allows you to use all sorts of lovely Bluetooth accessories with your computer. 

PalmOne GPS Navigator
This Bluetooth GPS kit for the Tungsten T3 and Zire 72 comes with everything you'll need to hit the road. It uses TomTom navigation software and TeleAtlas maps. 

Think Outside Stowaway Universal Bluetooth Keyboard
The ever-popular Stowaway XT has gone Bluetooth. A great keyboard, and Bluetooth allows you to place the PDA where you wish. Supports Bluetooth enabled Pocket PCs, Symbian Series 60 phones and the Sony Ericsson P800/P900. 

RoboForm
Tanker Bob takes an in-depth look at RoboForm which allows you to organize and store secure data on your Palm. It has both desktop and Palm OS applications which allow you to keep your sensitive data safe and handy. 

BackupBuddy for Windows
Tanker Bob takes a look at one of our long-standing heroes, which offers great power and flexibility in Palm to Windows backups. 

FAQs & How-to's:

- Palm vs. Pocket PC**
- Windows Mobile 2003 SE Comparison**
- Pocket PC 2003 Comparison**
- Moving from Palm to PPC and vice versa**
- Mac FAQ**
- Wireless Internet**
- How to Evaluate a GPS**
- WiFi / 802.11b Wireless**
- How Much RAM do you Need?**

General PDA FAQ

All FAQs & How-to's

Free Pocket PC Themes

Game Reviews

http://web.archive.org/web/20041115011708/http://www.pdabuyersguide.com/

66

DIRECTV Exhibit 1017

EXHIBIT A



HP iPAQ 6315 Pocket PC Phone: The long wait is over and the 6315 is finally here with service from T-Mobile in the US. This device is both a cell phone and a Pocket PC running Windows Mobile 2003 Phone Edition. It packs a trio of wireless with GSM, WiFi and Bluetooth, has a VGA camera and a removable thumb keyboard. An excellent unit!
[Read the review.](#)



Sony Vaio U50 & U70: You may have read about the OQO and Vulcan Flipstart ultra-personal PCs, but Sony beat them to it, releasing the latest U series PCs. Imagine combining the form factor and touch screen of a PDA with a Windows XP notebook and you've got the U50 and U70 which feature Celeron and Centrino processors, enough RAM to get you working and ports to connect to your favorite peripherals. And don't forget the embedded WiFi 802.11g and wired Ethernet! These Japanese models are available from importers and cost \$2,200 to \$2,700.
[Read the review.](#)



Dell Axim X30: The first line of Pocket PCs running the new Windows Mobile 2003 Second Edition OS on an Intel PXA270 Bulverde processor are here. There are three X30 models, and two of them have both Bluetooth and WiFi. The top model has a screaming 624 MHz processor! As always, these Dells are priced right. We review the 312 and 624 MHz wireless models.
[Read the review.](#)



HP iPAQ rx3115: The rx3000 models are part of HP's Digital Entertainment Pocket PC model line targeting consumers who want multimedia features and good performance. The 3115 is the base rx model but brings a lot to the table for \$349: it runs Windows Mobile 2003 SE, has Bluetooth, WiFi, Nevo AV remote, a sharp display and great sound.
[Read the review.](#)



Handspring Treo 600: Those of you who've been patiently waiting: the Treo 600 is here! Available on the Sprint PCS and GSM networks, the Treo 600 is a feature-rich Palm OS smartphone with an integrated VGA camera, thumb keyboard and a bright color display. It runs Palm OS 5 and has a fast 144 MHz processor.
[Read the review.](#)

Over 200 Reviews!

Palm OS Games
Pocket PC Games
Linux PDA Games

Latest Palm:
Tantric
Equilibria
Fish Tycoon
Legacy
Warfare Incorporated
MicroQuad
Sega Action Games

Latest Pocket PC:
Octopuzzle
Creepy Pinball
Podz
Street Duel
Sky Force
Warfare Incorporated
Age of Empires

* All product logos and product names are property of their respective owners.

* The products referenced on this site are manufactured and sold by parties other than pdabuyersguide.com. PDAgroove/pdabuyersguide makes no representations regarding either the products or any information vendors offer about their products. Any questions, complaints, or claims regarding the products must be directed to the appropriate manufacturer or vendor. Copyright © 1998-2004 PDAgroove. All rights reserved. The graphical images and content on this web site are for private use only. All other rights-including, but not limited to, use on other websites, distribution, duplication, and publishing by any means - are retained by PDAgroove. Federal law provides criminal and civil penalties for those found to be in violation.

* Read our Privacy Policy.



[PDA](#) [Smartphone](#) [Notebooks](#) [Gaming](#) [Accessories](#) [Software](#) [Shop](#) [Discussion](#)

PDA reviews, phone reviews, Tablet PC reviews, game reviews and more!

Advertisement

HP iPAQ rx3115 Pocket PC

Posted September 18, 2004 by Lisa Gade, Editor in Chief

With its Fall 2004 Pocket PCs, HP has differentiated their iPAQs into three product lines, Digital Entertainment iPAQs, Classic Performance iPAQs and the [iPAQ 6315](#) Pocket PC phone. The iPAQ [rz1715](#) and the rx3000 series models comprise the Digital Entertainment iPAQs, and these target consumers. Here in the US, there are three models, the rx3115, rx4314 and [rx3715](#). Though the rx3415 appears only in HP's US specs pages and not on their main site so we're not sure if it will be available here. The camera-less rx3115 seems to target the US market and hasn't been announced for Europe or Asia, likely because of US corporate rules about cameras in the workplace and even public schools.

The rx3115 is a very good unit for the money, offering strong performance, Bluetooth, WiFi and the ever-popular Nevo AV remote. In fact, all the Fall 2004 iPAQs except the rz1715 have both WiFi and Bluetooth. Like the rz1715, it sports HP's new and not very sexy design, but unlike the rz1715, the 3115 does offer a nice set of features for the price. At \$70 more than the entry level rz1715, the rx3115 brings a lot to the table, adding a faster processor, Bluetooth, WiFi, more RAM, a user replaceable battery and Nevo. If you can spare the change, the rx3115 is definitely the better buy.



In the Box

The iPAQ rx3115 comes with a replaceable Lithium Ion battery, world charger, USB sync cable (not cradle), stylus, earbud headphones, case, software CD and several manuals including a thick "Special Features of the rx3000 series" manual which covers the bundled multimedia software in depth.

Features at a Glance

The iPAQ rx3115 is a compact device that has a 3.5" QVGA transfective display, an SD slot supporting SDIO, WiFi, Bluetooth and consumer grade IR. It runs Windows Mobile 2003 Second Edition (SE) with native support for both portrait and landscape modes, has a 300MHz processor and ~56 megs of total available memory. Unlike its bigger rx brothers, the 3415 and 3715, it doesn't have a digital camera.

Design and Ergonomics

While the rx series doesn't have the style and curvy good looks of the last generation iPAQ 1945 and 4150 models, it

Deals and Shopping!



[HP iPAQ RX3115 Pocket PC](#)
Hewlett Packard
Best Price \$189.00
or Buy New
[Buy amazon.com from](#)
Privacy Information

Compare Prices on the Hewlett Packard iPAQ RX3115

Stores	Prices
HPShopping	\$279.99 Shop Now!
Newegg.com	\$319.99 Shop Now!
Crutchfield	\$349.99 Shop Now!
PC Connection	\$349.95 Shop Now!
eCOST.com	\$307.95 Shop Now!

[See all 24 deals \(\\$270-\\$382\)](#)
[Shop for other PDAs](#)

Questions? Comments?
[Post them in our Discussion Forum!](#)

[View our Windows Mobile 2003 SE Comparison Matrix](#)

EXHIBIT A

isn't bad looking either. It's thicker than the rz1715 and the wider, shiny black side insets do much to balance the device's angular silver and black front face. The unit is compact for a Pocket PC, and as you can see from our comparison photo, it's one of the smallest Pocket PCs. All rx3000 models use the same casing and are the same size, they vary only in color.



Above: the palmOne [Tungsten T3](#), [ASUS A716](#), [Dell Axim X30](#) and the iPAQ

The device has a clean design, and the only button you'll find on the sides is the record button on the upper left. The SD slot is located on top as are the IR window, power button, headphone jack and stylus. On the front you'll find an LED that indicates wireless radio status and another for charging status and reminders. The iPAQ has a 5-way directional pad flanked by two buttons on each side. By default, these buttons launch, from left to right: iPAQ Mobile Media, HP Image Zone, Nevo AV remote and iTask. On most other Pocket PCs, these buttons launch the PIM apps, but since this is a multimedia oriented device, HP went with their multimedia apps. As with all Windows Mobile devices, you can re-map the buttons to launch any application you wish, and as with all 2003 SE devices, you can specify which applications are launched when the buttons are pressed and held for a second or two.

The removable Lithium Ion battery lives under a large door on the back of the unit, and the (loud) speaker seems to be located under the d-pad. As you'd expect, the sync connector is on the bottom edge, and it's the same connector as the iPAQ 3000, 5000, 2200 and 6315 models. For example, my iPAQ 5555 charger works with the rx3115 as does my iPAQ 6315 cradle. HP now refers to this as the universal connector, but don't confuse it with palmOne's universal connector, because they are different!

Display and Sound

The rx3000 series iPAQs use the same display and it's very bright, colorful and sharp. It has a neutral color bias and is perfect for viewing photos and watching movies. It has a 3.5" QVGA (240 x 320) transfective display, which are standard specs for Pocket PCs.

Sound is great on the rx3115 and all the rx3000 series models, as it should be for a multimedia-oriented device. The iPAQ is quite loud and you'll be able to hear movies, alarms and music in rooms with average or a bit higher than average noise levels. Like all Pocket PCs, the iPAQ has a standard 3.5mm stereo headphone jack, and unlike all, the unit comes with a set of earbud headphones. Sound quality is excellent through headphones and the volume is plenty loud. The iPAQ Audio control panel allows you to control headphone treble and bass as well as set microphone AGC (automatic gain control). All Pocket PCs have a mic and voice recorder, and the iPAQ is no exception.

WiFi

All Fall 2004 iPAQs (rx3000 series, hx4700 and the 6315) except the entry level iPAQ rz1715 have both WiFi and Bluetooth wireless networking. All use HP's new iPAQ Wireless as your one stop application for managing these wireless radios and their connections. The large round buttons turn each wireless radio on and off, and the other buttons allow you to manage each wireless connection's settings.

The iPAQ rx3115 has built-in WiFi 802.11b wireless Ethernet networking. It has very good range even though it doesn't have an external antenna. The iPAQ uses the Windows Mobile Connection Manager (a part of the OS) to manage wireless connections, and the device supports 64 and 128 bit WEP encryption, 802.1x using PEAP, SmartCard or Certificates. It comes with the Windows Mobile Certificates applet for managing certificates. The connection worked reliably for us when connecting to access points (with and without WEP) and worked seamlessly with iPAQ Mobile Media.



iPAQ Wireless is where you'll manage your WiFi and Bluetooth radios and connections.

Bluetooth

The iPAQ uses HP's Bluetooth Wizard which is powerful and user-friendly. It walks you through connecting to a variety of devices, from your ActiveSync partner (if you have a USB Bluetooth adapter installed on your PC), to mobile phones to access points and GPS units (it doesn't support Bluetooth headsets). The Bluetooth software is made by Widcomm and is version 1.5.0. I ActiveSync-ed wirelessly, connected to [Belkin](#) and [Red-M](#) Bluetooth access points for Internet access and transferred files to other Bluetooth enabled Pocket PCs.

Horsepower and Performance

The iPAQ runs a 300MHz Samsung S3C 2440 processor and has 56.66 megs of RAM available (about 10 megs of that is used by the OS and at least another 9 must be allocated to running programs). 3.91 megs of persistence NAND flash memory is available as the iPAQ File Store. The unit feels fast and responsive in all tasks, and should satisfy most users. I'd like to see more RAM, but the unit is positioned at the bottom of mid-level Pocket PCs and more RAM would perhaps raise the price. The

	HP iPAQ 1945 (2003, 4266MHz)	Dell Axim X30 312Mhz	HP iPAQ rz1715 (203MHz)	HP iPAQ rx3715 (400MHz)	HP iPAQ rx3115
Spb Benchmark index	1335	1474	1031	1545	1211
CPU index	1307	1673	1010	1529	1197
File system index	1184	1050	945	1387	1082
Graphics index	2774	3916	1783	2956	2372
Platform index	1291	1142	960	1422	1131
Write 1 MB file (KB/sec)	993	1030	755	1422	1058
Read 1 MB file (MB/sec)	22.7	28.6	19.2	23	18.8

EXHIBIT A

Samsung processor is ARM and XScale compatible so existing Pocket PC software will run fine.

How about video playback? Using the bundled PocketTV Pro to play "The Chosen" (a neat BMW flick with Clive Owen) which is a 4:26 minute long, 10 meg MPEG1 file recorded at 320 x 240, 308 kb/s, the iPAQ managed a respectable 24.96 fps. [PocketMVP](#) played "The Chosen" at 23.98 fps, and dropped 5 out of 6394 frames. The rx3115 played the Spider Man trailer file commonly found on the web (240 x 136, 452Kb/s encoded MPEG 1 file) at 23.98 fps and dropped only 2 out of 2640 frames. My own test MPEG1 file burned from a DVD at a whopping 700 Kb/s looked OK in playback with some occasional stuttering, which is good for a Pocket PC below 400MHz. It played back at 16.88 fps using PocketMVP and 23.6 fps using PocketTV Pro. If you want to play videos encoded at very high bitrates, consider the iPAQ [rx3715](#) which handles that task well.

Gaming is also pleasant on the device and most all of the current popular games we tested ran well. If you're into emulators, you will likely want the fastest device you can afford, but if you're a casual to moderate gamer, the 3115 is adequate.

Benchmarks

We performed benchmark tests using Spb Benchmark, which has become the standard for testing Pocket PC performance. The iPAQ did well for a 300MHz device, but surprisingly didn't post great improvements over the 266MHz [iPAQ 1945](#). HP's older intro level model running Windows Mobile 2003. Of course, the iPAQ rx3715, being a 400MHz device, did the best overall. The 3115 holds its own against the 312MHz [Dell Axim X30](#), which also sports dual-wireless and a compact form factor. The Dell lacks HP's multimedia software bundle, so if you're into MP3s and video and like the sound of the software described below, do consider this iPAQ.

Battery

The iPAQ comes with a user replaceable 920 mA Lithium Ion battery. That's an average size battery that should make it a few days on a charge. If you're a serious WiFi or Bluetooth user, or watch a lot of movies, you might want to consider the iPAQ 3715 which has a 1,440 mA battery or HP's optional 1,440 or 2,880 mA extended batteries (\$69 and \$129).

Copy 1 MB file (KB/sec)	993	1029	746	1392	1041
Write 10 KB x 100 files (KB/sec)	785	705	586	1066	796
Read 10 KB x 100 files (MB/sec)	9.65	9.51	7.98	10.2	8.18
Copy 10 KB x 100 files (KB/sec)	748	629	560	960	721
Directory list of 2000 files (thousands of files/sec)	33.3	19.8	27.4	37	29
Internal database read (records/sec)	1024	1280	835	1329	1004
Graphics test: DDB BitBit (frames/sec)	407	308	238	388	313
Graphics test: DIB BitBit (frames/sec)	20.4	21.4	13.5	29.8	22.1
Graphics test: GAPI BitBit (frames/sec)	427	913	272	392	325
Pocket Word document open (KB/sec)	48.1	36.1	92.5	54.6	42.3
Pocket Internet Explorer HTML load (KB/sec)	9.76	6.73	4.82	10.2	7.98
Pocket Internet Explorer JPEG load (KB/sec)	187	206	71	220	169
File Explorer large folder list (files/sec)	715	592	568	763	619
Compress 1 MB file using ZIP (KB/sec)	268	230	207	312	240
Decompress 1024x768 JPEG file (KB/sec)	393	501	297	551	417
Arkaball frames per second (frames/sec)	157	262	112	158	127
CPU test: Whetstones MFLOPS (Mop/sec)	0.057	0.059	0.043	0.084	0.062
CPU test: Whetstones MOPS (Mop/sec)	37.2	43.2	28	55.2	41
CPU test: Whetstones MWIPS (Mop/sec)	3.66	3.88	2.76	5.44	4.02
Memory test: copy 1 MB using memcopy (MB/sec)	49.6	115	50	59.5	48.6

EXHIBIT A**Software Bundle**

The rx3000 series comes with generous compliment of multimedia software. You get HP Image Zone, comprised of a desktop app and a Pocket PC app that allows you to view, edit and send photos via email, HP Instant Share E-Mail and IR. HP Image Transfer is for automatic transfer of photos and video from your HP iPAQ to your PC using ActiveSync. It works with any ActiveSync method (USB, Bluetooth and Wi-Fi). It's really intended for rx models with digital cameras, but HP bundles it with the rx3115 as well. Of course, you get the "iPAQ Entertainment" Today Screen plugin which replaces the standard Today Screen view with large buttons for Mobile Media, Photos and Home Control (Nevo AV Remote). This is HP's new standard for their multimedia units, but you can uncheck it from your Today Screen settings if you wish to use the regular Today Screen. It's great if you mainly use the iPAQ for these multimedia apps, but likely most of us will also use the core Pocket PC functions and want quick access to calendar, tasks and other handy Today Screen info. HP's iTask, a nice task switcher, is also included. HP's iPAQ Backup (a re-branded version of the excellent Sprite Backup 3.0) is included in ROM and will backup either your PIM info or all iPAQ data to an SD card. The HP Mobile Printing app is included in ROM too, and this will allow you to print to a Bluetooth, IR or networked printer. 3rd party software includes the excellent PocketTV Pro MPEG1 movie player which is installed in ROM, as is Ilium Software's Dockware, which functions like a screen saver and displays photos and a calendar when the iPAQ is turned on but you're not using it.

ActiveSync 3.7.1 for the desktop is included, as is Outlook 2002. All Windows Mobile devices use ActiveSync to sync to desktops and sync PIM data to and from Outlook. If you have a newer version of Outlook, you can use that instead of the version included on the CD.



HP Image Zone

iPAQ Mobile Media Player and Nevo Software

HP's iPAQ Mobile Media (powered by Nevo) allows you to listen to MP3s, view photos and watch videos stored on the Pocket PC. It supports Windows Media format video files (.WMV), MP3s and images (JPEG, BMP, GIF, PNG and local TIFF files). The Windows XP-only desktop apps, NevoMedia Player and Server, work with iPAQ Mobile Media on the Pocket PC to allow you to manage and play music, pictures, and video through your wireless home network— very cool. You can also wirelessly transfer your digital music, photos, and videos from your networked PC(s) running NevoMedia Server to your iPAQ and take them with you. The iPAQ app has a Media Control function that allows you to control movie, photo and music playback on any Windows XP machine running the player app on your network. You can also stream movies to the Pocket PC and view photos stored on a machine running the server.

All worked well when we used the iPAQ to control music, image and video playback on a networked PC running Windows XP Pro, and we were able to copy multimedia files from the PC running the server to the iPAQ. However the iPAQ player won't play MP3s via a streaming connection (yuck), and won't play Windows Media movies streamed from the server if they have any form of copy protection. Playing non-copy protected content via streaming media, we got sound but no video. The manual says that streamed WMV files must be formatted specifically for the iPAQ in order to playback, but gives no information on what that means exactly. The same movies do play fine when stored locally on the iPAQ. A shame, if this unit could stream MP3s and all WMV files of 320 x 240 size or less, it would be much cooler.

Last but not least, there's the ever-popular Nevo AV remote, which keeps getting better. Nevo is a powerful AV remote app that will allow you to control pretty much every piece of home AV equipment on the market. It controls TVs, VCRs, DVDs, CDs, amps, tuners, cable boxes, satellite dishes and more. The list of supported brands is amazing, and the interface is unique yet very intuitive. You can set up multiple rooms and switch among them, so you can control your living room AV gear, bedroom stereo and TV, and so on.

Comparing the rx3115 and rx3715

Both units have the same physical design and casing. In fact, they look identical other than the color (the 3115 is silver while the 3715 is graphite). They use the same display, offer the same multimedia features and have the same sound quality and overall volume. How do they differ? The 3715 adds a 1.2 megapixel digital camera, more File Store memory and a 400MHz Samsung processor while the 3115 has a 300MHz Samsung processor. The rx3715 sells for US \$499, while the rx3115 is \$349.

Conclusion

A very nice Pocket PC at a good price. If you're looking for an entry to mid-level PDA with a great screen, nice multimedia software, and good performance, do consider the rx3115. The Nevo AV remote and consumer IR are a big plus and the dual wireless will help keep you connected. If you have a hankering for a camera, also consider the iPAQ rx3715.

Pro: Great display, excellent sound, good performance and dual wireless. WiFi has great range and HP's Bluetooth software (Widcomm) is as always, solid and user friendly.

Con: Could use more RAM, though you can use storage cards to expand the unit. Battery capacity is a bit lower than we like, though you can buy additional higher capacity batteries.

Web Site: www.hp.com

List Price: \$349

Specs:

Display: Transflective TFT color LCD, 64K colors. Screen Size Diag: 3.5", resolution: 240 x 320.

Battery: Lithium Ion rechargeable. Battery is user replaceable. 920 mA.

Performance: 300MHz Samsung S3C 2440 processor. 64 MB built-in RAM (~56 megs available). 3.91 megs available in File Store for your use.

Size: 4.5 x 2.8 x 0.64 in . Weight: 5.1 oz.

EXHIBIT A

Audio: Built in speaker, mic and 3.5mm standard stereo headphone jack. Voice Recorder and Windows Pocket Media Player 9 included for your MP3 pleasure.

Networking: Integrated WiFi 802.11b and Bluetooth 1.1.

Software: Windows Mobile 2003 Second Edition Professional operating system. Microsoft Pocket Office suite including Pocket Word, Excel, Internet Explorer, and Outlook. Also, MSN Instant Messenger for Pocket PC, MS Voice Recorder as well as handwriting recognition. 3rd party and HP software: iPAQ Wireless, Bluetooth Manager, HP Mobile Printing, iPAQ Entertainment (custom Today Screen plug-in with shortcuts to digital imaging and entertainment applications), iPAQ Mobile Media, Nevo Universal Remote, Pocket TV Pro, iPAQ Backup, HP Image Zone for iPAQs, Ilium Dockware Personal Edition. ActiveSync 3.7.1 and Outlook 2002 for PCs included.

Expansion: 1 SD (Secure Digital) supporting SDIO and SDIO *Now!*. Can NOT use iPAQ expansion sleeves.

In the Box: AC adapter, USB sync cable, stylus, carrying case, stereo earbud headphones, manuals and software CD.

[Back to MobileTechReview.com Home](#)

Questions? Comments? [Post them in our Discussion Forum!](#)

EXHIBIT A

W4: Second Workshop on Human Computer Interaction with Mobile Devices

31 August 1999, Edinburgh, Scotland

Call for papers



Aims and objectives

The last 3-4 years have seen the development and marketing of a vast array of mobile computing devices. These systems herald what we believe to be a new era of 'ubiquitous' computing. The utility of these devices is reduced by the problems of accessing information resources through tiny displays. This can be especially problematic where that information is 'perishable'; where its value is only relevant to particular locations and times. The utility of mobile devices is further reduced by the problems of manipulating miniaturised versions of 'standard' keyboards and pointing devices. Users are also forced to perform numerous, delicate operations by selecting very small icons. This workshop will provide a forum for academics and practitioners to discuss the challenges and potential solutions for effective interaction with mobile systems and builds on the success of the [First Workshop on Human Computer Interaction with Mobile Devices](#) held in Glasgow in May 1998. The workshop is intended to cover not only PDAs but also voice terminals, smart phones and laptops.

Attendance will be limited in order to encourage interaction. It will be possible for people to attend the workshop even though they have not submitted a paper.

Registration

You can register for the workshop using the normal INTERACT registration form. This is [available in the PDF file of the Advanced Programme](#) on the [INTERACT Web pages](#). The [advanced programme](#) incorrectly says that you cannot attend a workshop if you are not registered for the whole conference. You can attend for the Workshop only, it just costs a little more. The costs are:

	Conference delegates	Workshop only attendees
1 Day Workshop	Conference fee + £40	£80

Please use the code W4 for the workshop.

Workshop Timetable

As we had so many good submissions we have accepted 11 papers and 6 posters. Our draft plan for the workshop is below. This is likely to change as we go along but it will give you an idea for what we hope the day will be about. Each author will get 30 minutes to present his/her work: 15 - 20 minutes of presentation and 15 - 10 minutes of discussion.

Over lunch and coffee breaks we will run a poster session in a break-out room near the main workshop room. The authors of the posters will be there to present them over coffee breaks but the posters will be up all day for people to look at during lunch. We hope that the long lunch and coffee breaks will lead to considerable discussion amongst attendees as we received too many papers to allow in meeting discussion bar through questions.

Papers are available in postscript format either individually or in two grouped zip archives: [papers.zip](#) and [posters.zip](#) 1340K and 725K

Note: there appears to be a problem with PDF conversion to postscript with these pages. PDF submitted files are also available in original PDF and in [eratum.zip](#). Sorry for the trouble but I don't have time just now to investigate further or convert all to PDF, Mark.

Draft Timetable	
08:45	Registration

EXHIBIT A

<p>09:10 - 10:45</p>	<p>Paper Session 1: Input/Output 1</p> <p>Applying Perceptual Layers to Colour Code Information in Hand-Held Computing Devices. Deshe, O & Van Laar, D. (University of Portsmouth, UK) 240K</p> <p>Dictionary based text entry method for mobile phones. Dunlop, M. D. & Crossan, A. (University of Glasgow, UK) 414K</p> <p>The Finger-Joint Gesture Wearable Keypad. Goldstein, M. & Chincholle, D. (Ericsson Radio Systems, Sweden) 3132K</p>
Coffee and Posters	
<p>11:15 - 12:15</p>	<p>Paper Session 2: Context of use</p> <p>A diary study of information capture at work. Brown, B., O'Hara, K. & Sellen, A. (Hewlett-Packard Labs, Bristol) 79K also PDF</p> <p>Implicit human-computer interaction through context. Schmidt, A. (University of Karlsruhe, Germany) 252K also PDF</p>
Lunch and Posters	
<p>13:45 - 15:15</p>	<p>Paper Session 3: Input/Output 2</p> <p>Comparison of speech input and manual control of in-car devices while on the move. Graham, R. & Carter, C. (HUSAT Research Institute, University of Loughborough, UK) 212K</p> <p>Mobile asynchronous communication: Use and talk of use among a group of young adults in Finland, 1999. Koskinen, T. (Nokia Mobile Phones, Finland) 233K</p> <p>Extending the auditory display space in handheld computing devices. Walker, A. & Brewster, S. (University of Glasgow, UK) 371K</p>
Coffee and Posters	
<p>16:00 - 17:30</p>	<p>Paper Session 4: Design</p> <p>Research Methods Used to Support Development of Satchel. Eldridge, M., Lamming, M. Flynn, M., Jones, C. & Pendlebury, D. (Xerox Research Centre Europe, UK) 274K also PDF</p> <p>Coping with consistency under multiple design constraints: the case of the Nokia 9000 WWW browser. Hjelmeros, H., Ketola, P. & Raiha, K-J. (Nokia and University of Tampere, Finland) 986K</p> <p>Design challenges of an In-Car Communication System UI. Koppinen, A. (Nokia Mobile Phones, Finland) 146K</p>
Pub	
<p>The Posters</p> <p>The Digital Dictaphone: an exercise in audio-only interaction design. Barfield, L. (University of the West of England, UK) 124K</p> <p>Places to stay on the move: software architectures for mobile user interfaces. Dix, A., Ramduny, D., Rodden, T. & Davies, N. (aQtive Ltd, University of Staffordshire, University of Lancaster) 1632K</p> <p>Mobile computers in a Community NHS Trust. Is this a relevant context and environment for</p>	

EXHIBIT A

[their use?](#) *McManus, B. (University of Central Lancashire, UK) 231K*

[A Graphical Interface for Wearable Computing.](#) *Newman N. & Clark, A. (University of Essex, UK) 493K*

[Using mobile communication devices to access virtual meeting places.](#) *Rist, T. (DFKI, Germany) 939K* [also PDF](#)

[A personal digital assistant as an advanced remote control for audio/video equipment.](#) *De Vet, J. & Buil, V. (Philips Research, The Netherlands) 1024K*

As we had so many papers we have decided to do away with the idea of discussion groups to get more papers and posters in.

Information for Authors

The closing date for paper submissions has now passed. We received a very pleasant 25 submissions - for more than could be accepted for a one day meeting, making the reviewing process rather more difficult than we imagined.

At the workshop, 3-5 page extended abstracts will be distributed as a draft proceedings as submitted. Each author will get 15-20 minutes to present his/her work followed by 15-10 minutes of questions and discussion. Please design your talk to fit within 20 minutes maximum, because of the number of papers we have limited scope for in meeting discussion - it is very important we do not lose these discussion slots.

The proceedings of the workshop will be published in the journal *Personal Technologies*. Authors of accepted papers and posters will be asked to resubmit for the journal by 31 October 1999.

Contact and more informationStephen Brewster

Department of Computing Science,
University of Glasgow,
Glasgow G12 8QQ, Scotland.

e-mail: stephen@dcs.gla.ac.uk

phone: +44 (0)141 330 4966

fax: +44 (0)141 330 4913

Programme Committee

Joint programme chairs: [Stephen Brewster](#), University of Glasgow, and [Mark Dunlop](#), Risø Danish National Laboratory.

[Peter Brown](#), University of Kent.

Elisa Delgado, [Cambridge Technology Partners](#).

Mikael Goldstein, [Ericsson](#)

[Phil Gray](#), University of Glasgow.

Steve Hodges, [ORL](#).

[Chris Johnson](#), University of Glasgow.

[Matt Jones](#), Middlesex University

[Peter Johnson](#), QMW.

Bruno von Niman, [Ericsson](#)

Judith Ramsay, [Nortel Networks](#)

Satu Ruuska, [Nokia](#).

[Meurig Sage](#), University of Glasgow

[Peter Thomas](#), University of The West of England.

Last updated 17/August/99

EXHIBIT A

This meeting is jointly organised by the Glasgow Interactive Systems Group, the British HCI group and the INTERACT 99 Conference.



Partly supported by EPSRC Grant GR/L66373.

EXHIBIT A

http://web.archive.org/web/20030314065918/http://www.dcs.gla.ac.uk/mobile99/papers/de_vet.ps

A personal digital assistant as an advanced remote control for audio/video equipment

John de Vet & Vincent Buil

Philips Research
Prof. Holstlaan 4
5656 AA Eindhoven
The Netherlands

Email: {devet , builv}@natlab.research.philips.com

This paper describes a personal digital assistant that is used as a catalogue and advanced remote control to browse, select and play music in a compact disc jukebox. The application has been developed as a research prototype to identify advantages and disadvantages of different interaction styles for accessing large amounts of content. The basic concept provides easy access to a personal music catalogue, anywhere and anytime. It also allows you to control the CD jukebox. It employs a multimodal interaction style which combines voice control, touch input, visual output with animations and functional sounds. This helps to overcome the typical problem of accessing large information resources through small displays. In addition, redundancy in both input and output techniques offers people alternative ways of interacting with the content. The concept will be described and demonstrated, and relevant user studies will be explained.

Keywords: personal digital assistant, multimodal interaction style, voice control, compact disc jukebox, usability evaluation, personalisation

1. INTRODUCTION

A mobile personal device such as a personal digital assistant (PDA) provides good options to access large amounts of information and entertainment content anywhere and anytime. This paper describes a PDA that is used as a catalogue and advanced remote control to browse, select and play music tracks in a compact disc jukebox. The application has been developed as a research prototype to identify advantages and disadvantages of different interaction styles for accessing large amounts of content. It can also be used as a basis for identifying options for personalisation.

The basic concept employs a multimodal interaction style which combines voice control, touch input, visual output with animations, and functional sounds. The inclusion of both voice input and functional sounds helps to overcome the typical problem of accessing large information resources through small displays. Also, redundancy has been built in, in both input techniques as well as output techniques. This offers people alternative ways of interacting with the content, depending on context of use demands, on personal preferences, or on what is deemed socially appropriate. For example, selections

can be made by tapping an item in a list using the stylus, or by speaking the item's name directly. The last alternative would require a quiet environment, whereas the first alternative can be used in noisy environments.

The concept will be described and demonstrated, and relevant user studies will be explained

2. THE CONCEPT

A personal digital assistant is a handheld device that combines computing, communication, and networking features. It is typically pen-based, using a stylus rather than a keyboard for input, and offering handwriting recognition features. Some PDAs, such as the Philips Nino (Philips 1999), can also react to voice input by using voice recognition technologies.

The Philips Nino 300 has been used as a catalogue and remote control to select music compact discs in a personal CD jukebox. The CDs are shown in a list on the display of the PDA (see Figure 1). The list of CDs can be sorted by music style, artist name, release years and album names, by either using the stylus or voice commands. For example, the user can say

'Herbie Hancock', and the CDs of Herbie Hancock that are in the user's collection are shown on the PDA display. The first CD that is shown is highlighted. Simply saying 'play' results in activating the jukebox system to play the selected CD.



Figure 1: The PDA screen with the personal Jukebox user interface.

The information needed to create the CD catalogue on the PDA is simple: for each CD a number of attributes is available: artist, album, year, and style. This information can be downloaded from the Internet, for instance via CDDB, a feature that most audio CD players on the PC now offer (CDDB 1999). This means that the user does *not* need to enter this information manually, as is typically the case with current CD changers for the home. Ideally the jukebox system would send the ID information of the CDs to the PDA. Connecting the PDA to the PC would then result in an update of the catalogue. If the user has no connection to the Internet at home, it is still possible to enter the information (by typing on a PC keyboard, instead of pushing buttons on the changer).

The technology involved includes (see Figure 2):

- multimodal interaction (stylus gestures, voice input, animation, functional sound)
- Philips Vocon ASR software (continuous, word-based speaker dependent developed for small vocabulary and small 'footprint' (i.e. low memory & CPU resources) platforms, and hence cheaper devices.)
- infrared communication between PDA to PC via an IrDA (Infrared Data Association) link.

Figure 2: Set-up of PDA and PC simulation with IrDA transceiver on top of the left speaker.

- MP3 music on PC, meta-data from Internet. The CD changer is completely simulated on the PC using a modified Winamp MP3 player (Nullsoft 1999) and the CD collection is in MP3 format.

The following user benefits are anticipated:

- *Add-on remote control feature to an already bought product.*

A PDA is too expensive to be positioned as a personal remote control only, therefore the concept should be seen as an add-on feature. Existing universal remote controls, like are Marantz's RC2000 Mark II, Philips' Pronto and Sony's RM-AV2000, offer extensive and comparable control options. However, they do not offer the catalogue browsing option, which has been implemented on the PDA relatively easy.

- *Easy to use overviews of your CD collection on screen.*

The collection is shown on the display as a scrollable list of CD items, that can be sorted by music style, artist name, release year, or album title.

- *Using voice commands to access content directly.*

Music styles, artists, and release years can be named and immediately the associated subset of the collection will be shown on the display.

- *Browsing your CD catalogue anywhere and anytime.*

The catalogue can be shown to friends anywhere you are. Or you it can be consulted while shopping in your local CD store to see what you already have.

Anticipated user concerns are the following:

- *Getting the CD information on the PDA.*
This requires an Internet account to automatically download for instance CDDB information (CDDB 1999). The alternative would be for the user to manually type in the information. The catalogue in the current prototype is fixed and contained in a data file which can only be altered manually.
- *Adding a CD to your collection.*

Ideally, the catalogue could be updated when a new disc is inserted in the CD changer. Alternatively, the update of the catalogue would have to be done manually.

- *Training of voice commands.*
Current word-based speech recognition technology requires training of new words, for example when a new CD is added. In the long term, phoneme-based, speaker independent speech recognition would be the solution, but this technology is not yet available on PDAs.

The opportunities that have been identified are:

- *Allows both personal use and group use.*
A catalogue on a remote control can be used to find content of personal interest, without disturbing other people in the room who are using the audio/video equipment. The mobile device's display suits personal use. In case you want to enjoy audio or video together, i.e. for group use, a shared display (like a TV screen) would be better suited to find content of common interest.
- *Control multiple devices and a variety of content.*
The concept is also suitable for other applications, such as an electronic programme guide (EPG) that could be used as a personal TV programme recommender, or a catalogue of a videodisc (or videotape) collection. Hence it can offer access to a variety of content: music, TV programmes, film, theatre shows, sport events, and so on.
- *Hands-free control by voice.*
For the control of audio/video equipment by voice, one controversial issue is the microphone location, and thus on how the automatic speech recognition (ASR) should take place. A microphone in the set (e.g. CD changer) allows for hands-free operation, but this scenario is more prone to noise interference, in particular to 'noise' coming from the audio/video equipment itself. A microphone in the remote control improves the quality of recognition, but does not free the hands. In case of a PDA, with on-board ASR and a reasonable display, the benefit of good visual feedback can compensate for the lack of hands-free operation. (When solely used for control, the PDA can be placed on the table, in principle, but the recognition will deteriorate.)

3. RESEARCH QUESTIONS

The research questions we had regarding *the concept* were:

- How do people appreciate the concept of using their organiser as a (universal) remote control for their audio/video equipment?
- How do people appreciate the concept of talking to a mobile device in the home or away?

Our research questions regarding *the user interface* were:

- Which operations are easier to perform with speech commands, and which operations are easier to perform on a touch screen?
- How to design a multimodal interaction style for use in different contexts (in the home, on the move, and away)?
- An organiser is a personal device, and thus can become a personal remote control that does not need to be shared with others. How can personalisation be exploited?

4. USER STUDIES

Our research group has conducted many user studies on the use of voice control in combination with other input techniques, for both stationary and portable products in the home environment. We have been most interested in relating user's conceptual operations to appropriate input and output techniques. Some of the findings will be summarised here.

4.1 Voice control

Operations that favour voice control:

- *Direct addressing of content:* Calling out names (e.g. of artists, categories, channels, etc.) is by far preferred over entering names with cursor keys on a remote control, or scrolling through names in a long list. Using voice commands is more natural and faster, and has better conceptual mapping (i.e. channel names vs. channel numbers). Earlier studies confirm that this is one of the main benefits of voice commands (e.g. the 'name dialling' feature in some mobile phones). However, for word-based speech recognition the names need to be trained in advance.
- *Menu navigation & selection:* Navigating through menu structures and selecting options is faster and preferably done with voice commands, compared to navigating with the cursor keys on a remote control. The task can be performed faster as there is no need to navigate stepwise through an option list or menu structure, and no need to switch attention back and forth between remote control and screen. Navigation through menu structures can be even more powerful with 'power commands', i.e. short cuts to options deeper in the menu structure, or macro functions that perform several selections at once (i.e. 'record this CD').
- *Setting a range:* When people have to set points on a scale, for example the start and stop time of a TV programme to be recorded on videotape, then voice commands are easier and faster to use than cursor keys. Setting times

with voice commands requires fewer actions than setting times on a slider bar with the cursor keys.

4.2 Manual control

Operations that favour manual control:

- *Scrolling in a long list:* Cursor keys are preferred and work faster for scrolling through long lists of content, if one does not know what one is looking for (browsing). Repeated voice commands like 'up, up, up' are annoying and slow, especially if the target item requires a lot of scrolling. An advantage of push buttons is that they can be held down for continuous scrolling. An even better alternative would be a real slider button or a rotary knob, as it facilitates controlling the position and displacement directly.

4.3 Voice and manual control combined

In one experiment we compared three versions of a Jukebox interface: voice input only, manual input only, and voice combined with manual input. We found that switching between voice and manual input seems unnatural to some users.

However, a combination of both input techniques can be very useful. For example, in the CD jukebox application on the PDA users can select a CD with the stylus, and subsequently invoke the 'play' command by voice.

Another advantage of combining voice and manual input, is that it provides alternative ways of operating the device. When automatic speech recognition is cumbersome, e.g. in a noisy environment or when the device is trained by another person, the manual input is a fallback option. User tests show that people want to have this possibility. Our post-experiment questionnaire results show that people really would want to use manual control instead of voice control in the following situations:

- *personal context:* when one is not in the mood to talk to a device, not able to talk (e.g. one has a hoarse voice), or when it is inappropriate (e.g. during a concert or presentation).
- *social context:* when one is talking to others, or when you don't want to disturb other people in the room.
- *physical context:* when there is a lot of noise in the room – during a party for example – and voice control just doesn't work very well.

5 DISCUSSION AND FUTURE RESEARCH

The concept presented in this paper is a prototype of what could be an add-on remote control feature for

people who already own a PDA. The concept is suitable for other applications, such as an electronic programme guide (EPG) that could be used as a personal TV programme recommender, or a catalogue of your videotapes or videodiscs.

The disadvantages of mobile devices (small displays and few buttons, no keyboard) have been compensated by using voice input in combination with stylus input. Redundancy in the use of different input modalities makes it a robust interaction concept, that can be used in different contexts of use.

The real estate of the small display has been used in such a way that the items in the CD catalogue can be sorted on various attributes (artist, music style, release year), and sub-selections can be quickly made. In addition, animations and functional sounds have been added, to offer more redundancy in different output modalities.

This concept of a multimodal interaction style on a mobile device, seems also applicable to other domains than just entertainment, such as information and communication applications. It offers easy access to content through mobile devices. The mobile device does not necessarily store the content, although that would be possible, but it can be a gateway to that content, as exemplified by our application.

Our work has generated various questions for future research:

- *multi-user and multi-appliance:* A PDA is designed for personal use. How to design and implement voice control for use in a room with other people and other equipment?
- *shared interaction / scalability:* A single PDA does not support shared interaction: it is difficult to show your catalogue to others. A bigger screen that can be shared (e.g. a TV screen in the living room) is an option, but How well can a small-display application be scaled to a bigger displays?
- *personalisation:* Although the content, your CD collection, is personalised, the application and user interface are not. What are the options for personalising the personal remote control?

In the final paper, we will elaborate more on the experiments (design and data), on the advantages and disadvantages of the concept, and the implications for future research.

Acknowledgements

This work is a combined effort of our colleagues Vincent Buil, Berry Eggen, Luc Geurts, Paul Kaufholz, and Leon van Stuivenberg.

REFERENCES

CDDDB Online audio CD database (1999)
<http://www.cddb.com/>.

Philips Nino palm-PC official website (1999)
<http://nino.philips.com/>.
Nullsoft, Inc. Winamp music player (1999)
<http://www.winamp.com>

EXHIBIT A

EXHIBIT A

<http://web.archive.org/web/20050520171501/http://www.paradyne.com/products/6300/6300.pdf>



Product Data Sheet

6300 ADSL2+/ReachDSL Enhanced DSL CPE Family

6381, 6382, 6388

Bridge/Router, Multi-Port Switch, and WiFi Intelligent CPE Family

Overview

With Paradyne's innovative, easy to use ADSL/R CPE family, service providers can provide ADSL2+ service and ReachDSL service in the same unit, ensuring coverage to the entire subscriber base. The 6300 CPE family provides enhanced remote diagnostic tools that allow the service provider to remotely access this enhanced endpoint for quick trouble isolation in order to maintain the highest level of service.

The Paradyne 6300 enhanced CPE are easily user-installed. The embedded web-based user interface is designed to simplify ADSL deployment. All products provide an Ethernet connection that is auto-sensing, eliminating the worry about connection cable type (straight-through vs crossover). All units include a built in POTS filter that eliminates the expense of an external filter as well as reduces installation errors.

The 6300 enhanced CPE all default to a simple bridge. This and other default settings make for a quick and easy installation that doesn't require any configuration.

When operating in router mode, these gateways support DHCP Server/Relay/Client, NAT, as well as RIP, dynamic routing, port forwarding, static routing, and ping initiation. For security firewall functions including PAP (Password Access Protocol) and CHAP (Challenge Handshake Authentication Protocol) are supported.

The 6382 multiport Ethernet CPE and the 6388 multiport Ethernet CPE with wireless access incorporate an Ethernet switch rather than a hub and provide versatile solutions for the deployment of residential and business customers including packet voice and video services.

In addition all of the CPE that make up the 6300 family support the key OpIQ feature DELT to help service providers debug subscriber service issues. DELT, or Dual End Loop Test, is a feature that is present in Paradyne's ADSL2+ DSLAMs and BLCs and is also a feature of Paradyne ADSL2+ CPEs. Because DELT is a dual-ended test, it requires equipment that supports the DELT feature at both ends of the copper loop.

DELT is primarily used for reactive tests on a loop after a modem has been deployed—either to help troubleshoot a line or to capture a baseline of loop characteristics at the time of installation.



Features

- Revolutionary combination of standards based ADSL and ReachDSL on a single platform
- DELT - Dual Ended Loop Testing
- Automatically selects technology with best performance - ADSL, ADSL2, ADSL2+, or ReachDSL 2.2
- Speeds beyond 24 Mbps using ADSL2+
- Compatible with all DSLAMs providing standard ADSL, ADSL2, and ADSL2+
- Integrated telephone filter
- Bridge and router configurations
- Includes PPPoE and PPOA clients
- Includes Stateful Inspection Firewall, PAP, and CHAP for security
- DHCP Server/Client or proxy, dynamic and static routing
- Configured through easy-to-use web interface
- Includes both Ethernet and USB interfaces
- Supports 802.11b/g Wi-Fi and multiport routing
- Service provider pre and customizable default configurations
- Enhanced ping
- Telnet client

Benefits

- Enhanced service provider intelligent demarcation with remote diagnostics to streamline installation and simplify maintenance
- DELT - For integrated loop testing without external equipment
- Integrated WiFi 802.11b/g wireless access point provides universal coverage
- Single endpoint can be utilized for standard ADSL, ADSL2, ADSL2+ services as well as ReachDSL services
- Automatically switches to ReachDSL technology if line conditions do not permit acceptable service using standard ADSL, ADSL2, or ADSL2+
- Reduces number of truck rolls required to install and maintain services with customer self-installation and remote management
- Single modem for bridging and routing needs; defaults to bridge or to the pre-configured service provider options.
- Provides secure access with necessary authentication to give service providers a controlled and secure demarcation point between their network and customer's network
- Includes both USB and Ethernet interfaces for flexibility when installing
- Includes multiport Ethernet router with and without wireless access
- Integrated splitter and filter reduces installation costs and hassles

Specifications**Dimensions**

1.2" H x 6" W x 4.4" D (3.05cm H x 15.24cm W x 11.8cm D)

Weight

1.5lbs (shipping weight)

Power

100 VAC, 50 Hz
110 VAC, 60 Hz
220VAC, 50/60 Hz

Interfaces

DSL Line: RJ11
Phone: RJ11 (with integrated phone filter)
Ethernet: 10/100Base T, RJ45 (1 on 6210/6211, 4 on 6382/6388)
USB 1.1 (6381 only)
WiFi 802.11b/g (6388 only)

Standards Support

RFC 1483/2684 Multiprotocol Encapsulation over ATM
RFC 2364 PPP over ATM
RFC 2516 PPP over Ethernet
IPv4, TCP, UDP, ICMP, ARP, RARP, proxy-ARP
RIPv1, RIPv2
Static Routing
DHCP Server/Client/Relay
DNS Proxy
UPNP
Multicast: IGMP v1,v2 Snooping and Proxy
IEE 802.1d transparent bridging
Lookup table for 1K MAC Address

Security:

- NAPT
- Stateful Inspection Firewall
- PPP with PAP/CHAP
- 64/128/256-bit WEP Engine Encryption; PSK, TKIP;
- Shared Key Authentication
- Broadcast Storm Protection

ATM:

- Up to 8 PVCs, UBR, CBR, VBR
- OAM F5, F4 Loopbacks

Ordering Information

ADSL2+/ReachDSL Bridged/Routed CPE 10/100BaseT plus USB

6381-A3-200 ADSL2+/ReachDSL CPE Router (TI), 10/100BaseT, N.A.

6381-A3-210 ADSL2+/ReachDSL CPE Router (TI), 10/100BaseT, N.A., FCC Part 68 Approved

6381-A3-300 ADSL2+/ReachDSL CPE Router (TI), 10/100BaseT, U.K.

6381-A3-302 ADSL2+/ReachDSL CPE Router (TI), 10/100BaseT, EURO

6381-A3-304 ADSL2+/ReachDSL CPE Router (TI), 10/100BaseT, India

6381-A3-600 ADSL2+/ReachDSL CPE Router (TI), 10/100BaseT, Japan

ADSL2+/ReachDSL Bridge/Router 4 Port Ethernet Switch

Protocol Support

ANSI T1.413 (Full Rate ADSL)
ITU G.992.1 (DMT)
ITU G.992.2 (G.lite)
ITU G.992.3 (ADSL2)
ITU G.992.5 (ADSL2+)
ITU G.994.1 (G.hs)
ITU G.997.1
Paradyne ReachDSL 2.2

Management

Web based User Interface
Firmware Upgradeable via HTTP
Telnet Server
TFTP Server and Client
SNMP

Bandwidth/Distance

Downstream Speeds up to 24 Mbps using ADSL2+ (2.2 Mbps with ReachDSL)
Upstream speeds up to 2 Mbps with ADSL2+ (2.2 Mbps with ReachDSL)

Regulatory Compliance

FCC Part 68
FCC Part 15
CE
CUL
CS-03
TUV
ReachDSL 2.2 Spectral Compliance:
- ANSI T1.417
- ANSI T1.413
- UK ANFP
- ETSI TR101 830-1
- Approved for all loops in Japan by the TTC

Operating Requirements

Temperature: 32F to 104F (0C to 40C)
Non-operating temperature: -4F to 149F (-20C to 65C)
Humidity: 5% to 95%, non-condensing

EXHIBIT A

6382-A1-200 ADSL2+/ReachDSL CPE Router (TI), 4 Port Ethernet Switch, N.A.
6382-A1-210 ADSL2+/ReachDSL CPE Router (TI), 4 Port Ethernet Switch, N.A., FCC Part 68 Approved
6382-A1-300 ADSL2+/ReachDSL CPE Router (TI), 4 Port Ethernet Switch, U.K.
6382-A1-302 ADSL2+/ReachDSL CPE Router (TI), 4 Port Ethernet Switch, EURO
6382-A1-304 ADSL2+/ReachDSL CPE Router (TI), 4 Port Ethernet Switch, India
6382-A1-600 ADSL2+/ReachDSL CPE Router (TI), 4 Port Ethernet Switch, Japan
ADSL2+/ReachDSL Bridge/Router 802.11G WiFi plus 4 Port Ethernet Switch
6388-A1-200 ADSL2+/ReachDSL CPE Router (TI), 802.11G WiFi, N.A.
6388-A1-210 ADSL2+/ReachDSL CPE Router (TI), 802.11G WiFi, N.A., FCC Part 68 Approved
6388-A1-300 ADSL2+/ReachDSL CPE Router (TI), 802.11G WiFi, U.K.
6388-A1-302 ADSL2+/ReachDSL CPE Router (TI), 802.11G WiFi, EURO
6388-A1-304 ADSL2+/ReachDSL CPE Router (TI), 802.11G WiFi, India
6388-A1-600 ADSL2+/ReachDSL CPE Router (TI), 802.11G WiFi, Japan



For additional information on this or any Paradyne product or service, contact the office nearest you or dial 1.800.727.2396 (USA and Canada) or 1.727.530.8623; fax 1.727.530.8216. For international locations, visit the Paradyne web site at <http://www.paradyne.com>

[login](#)

[Compa](#) [Products](#) [Solutions](#) [Support](#) [News &](#) [Partners](#)

Technical Support

[Overview](#)

Documentation

[Manuals](#)

[Knowledgebase](#)

[Disc Notices](#)

Downloads

[Firmware](#)

[MIBs](#)

[Tools](#)

[Warranty Reg](#)

Service Programs

[Services Overview](#)

[Training Information](#)

[Repair & Warranty](#)

[Standard Service T&C](#)

SERVICE & SUPPORT

Bridge and Router Technical Manuals

- [ATM Endpoints](#)
- [IP Endpoints](#)
- [StormPort Modems](#)
- [TDM Endpoints](#)
- [Other Endpoints and RTUs](#)
- [POTS Filters and Splitters](#)

If you are looking for older versions of bridge and router technical manuals, [click here](#).

ATM Endpoints

[8300-A2-GB20-00](#) 4/03
Hotwire 8300 Endpoint User's Guide

[8300-A2-GN10-10](#) 6/03
Hotwire 8300 Endpoint Installation Instructions

[Go to Top](#)

IP Endpoints

[1740-A2-GB20-10](#) 9/04
1740 SHDSL 2/4-Wire Router User's Guide

[6205-A2-GZ40-10](#) 9/04
6205 ADSL Modem Installation Instructions

[6205-A2-GZ41-00](#) 7/04
6205 ADSL Modem Quick Installation Instructions

[6210-A2-GB23-00](#) 1/05
6210-A3 Bridge and 6211-A3 Bridge/Router User's Guide

[6210-A2-GZ13-00](#) 1/05
6210 Bridge and 6211 Bridge/Router Quick Installation Instructions

[6211-A2-GB21-20](#) 1/05
6211-I1 ADSL2+ Router User's Guide

[6211-A2-GZ10-10](#) 12/04
6211-I1 ADSL2+ Router Quick Installation Instructions

[6212-A2-GB22-00](#) 1/05
6212-A2 4-Port Router User's Guide

[6212-A2-GZ11-10](#) 12/04
6212 4-Port Router Quick Installation Instructions

[6218-A2-GB20-00](#) 2/05
6218-A1 Wireless Router User's Guide

[6218-A2-GZ10-00](#) 1/05
6218-A1 Wireless Router Quick Installation Instructions

[6300-R2-GB20-00](#) 3/02 (*Russian version*)
Hotwire DSL Routers, Models 6301/6302, 6341/6342, 6351, and 6371, User's Guide

[6300-A2-GB20-10](#) 11/03 (*English version*)
Hotwire DSL Routers, Models 6301, 6302, 6341, 6342, 6351, and 6371, User's Guide

[6301-A2-GN10-10](#) 3/01
Hotwire 6301/6302 IDSL Routers Installation Instructions

[6310-A2-GN10-60](#) 7/00 (*English version*)

[6310-B2-GN10-60](#) 8/00 (*French version*)

Hotwire MVL Modem, Model 6310-A3, with Inline Phone Filter, Installation Instructions

[6310-A2-GN12-00](#) 9/01 (*English version*)

EXHIBIT A

6310-B2-GN12-00	9/01	<i>(French version)</i>
Hotwire ReachDSL v1 (MVL) Modem, Model 6310-A4, with Inline Phone Filter, Installation Instructions		
6321-A2-GN10-00	3/00	
Hotwire 6321/6322 IDSL Routers Installation Instructions		
6341-A2-GN10-20	3/01	
Hotwire 6341/6342 SDSL Routers Installation Instructions (<i>also see</i> 6300-A2-GB20)		
6350-A2-GN10-10	12/00	<i>(English version)</i>
6350-B2-GN10-10	12/00	<i>(French version)</i>
Hotwire ReachDSL Modem, Model 6350-A3, with Inline Phone Filter Installation Instructions		
6350-A2-GN12-20	6/04	<i>(English version)</i>
6350-B2-GN12-10	4/02	<i>(French version)</i>
6350-R2-GN12-10	4/02	<i>(Russian version)</i>
Hotwire ReachDSL Modem, Model 6350-A4, with Inline Phone Filter Installation Instructions		
6351-B2-GN10-10	9/01	<i>(French version)</i>
6351-R2-GN10-10	9/01	<i>(Russian version)</i>
Hotwire 6351 ReachDSL Router Installation Instructions		
6351-A2-GN10-20	2/04	<i>(English version)</i>
Hotwire 6351 ReachDSL Router Installation Instructions (<i>also see</i> 6300-A2-GB20)		
6371-A2-GN10-40	9/01	
Hotwire 6371 RADSL Router Installation Instructions (<i>also see</i> 6300-A2-GB20)		
6381-A2-GB23-10	1/05	
6381-A3 Router User's Guide		
6381-A2-GZ13-00	12/04	
6381-A3 Router Quick Installation Instructions		
6382-A2-GB20-00	4/05	
6382 4-Port Router User's Guide		
6382-A2-GZ10-00	1/05	
6382 4-Port Router Quick Installation Instructions		
6388-A2-GB20-00	2/05	
6388-A1 Wireless Router User's Guide		
6388-A2-GZ10-00	1/05	
6388-A1 Wireless Router Quick Installation Instructions		
6390-A2-GK40-00	9/02	
Hotwire ReachDSL Modem, Model 6390, with Inline Phone Filter Installation and Operation Supplement		
6390-A2-GN10-10	9/02	<i>(English version)</i>
6390-B2-GN10-10	9/02	<i>(French version)</i>
6390-R2-GN10-00	5/02	<i>(Russian version)</i>
Hotwire ReachDSL Modem, Model 6390, with Inline Phone Filter Installation Instructions		

[Go to Top](#)

StormPort Modems

400 / 08-01137-01	9/00	
StormPort 400 Modem Installation Guide		
401 / 08-01139-01	9/00	
StormPort 401 eSled Modem Installation Guide		
405 / 08-01141-01	9/00	
StormPort 405 Modem Installation Guide		
600 / 08-01143-01	11/00	
StormPort 600 Modem Installation Guide		
610-A2-GN70-00	9/02	
StormPort 610 Modem Installation Sheet (<i>see note</i>)		
1020-A2-GN70-10	4/03	
StormPort 620 and 1020 Modem Installation Sheet (<i>see note</i>)		

Note: The 610, 620, and 1020 Installation Sheets are not designed for online viewing. Print them and fold them in thirds to use them as intended.

[Go to Top](#)

EXHIBIT A**TDM Endpoints**

7900-A2-GB21-20 12/01

Hotwire TDM SDSL Standalone Termination Unit, Models 7974-A2, 7975-A2, and 7976-A2, User's Guide

7900-A2-GN11-20 12/01 *(English version)*

7900-N2-GN11-20 12/02 *(Chinese version)*

Hotwire TDM SDSL Standalone Termination Units, Models 7974-A2, 7975-A2, and 7976-A2, Installation Instructions

7900-A2-GK40-00 12/00

Special Notice - Network Interface Option: Transmit Attenuation

7900-A2-GK41-00 12/00

Hotwire TDM SDSL Termination Unit Ferrite Choke Installation Instructions

7900-A2-GZ42-00 10/02

Hotwire TDM SDSL Standalone Termination Unit, Model 7974

Wall Mounting Installation Instructions

7990-A2-GB20-20 9/04

Hotwire TDM SHDSL Endpoints, Models 7995-A2-411, 7995-A2-421, 7995-A2-422, 7995-A2-700, 7996-A2-410, 7996-A2-420, and 7996-A2-700, User's Guide

7990-A2-GN10-20 9/04 *(English version)*

Hotwire TDM SHDSL Endpoints, Models 7995-A2-411, 7995-A2-421, 7995-A2-422, 7995-A2-700, 7996-A2-410, 7996-A2-420 and 7996-A2-700, Installation Instructions

7990-N2-GN10-00 12/02 *(Chinese version)*

Hotwire TDM SHDSL Endpoints, Models 7995-A1 and 7996-A1, Installation Instructions

7995-A2-GB21-00 9/04

7995-A2-374 SHDSL-Serial NTU User's Guide

7995-A2-GZ10-00 9/04

7995-A2-374 SHDSL-Serial NTU Quick Installation Instructions

7996-A2-GB21-00 9/04

7996-A2-374 SHDSL-G.703 NTU User's Guide

7996-A2-GZ10-00 9/04

7996-A2-374 SHDSL-G.703 NTU Quick Installation Instructions

[Go to Top](#)

Other Endpoints and RTUs

810_Installation_Manual 2/01

Allied Data CopperJet 81x ADSL Modem Installation Manual

810 / 4800-A2-GN13-00 9/02

CopperJet 810 Mounting Bracket Installation Instructions

4800-A2-GN14-00 5/03

Netopia Modem Mounting Bracket Installation Instructions

5216-A2-GN10-30 8/00

Hotwire 5216 RTU Customer Premises Installation Instructions

5246-A2-GN10-30 8/00

Hotwire 5246 RTU Customer Premises Installation Instructions

5446-A2-GN10-70 8/00

Hotwire 5446 RTU Customer Premises Installation Instructions

5620-A2-GN11-40 9/01

Hotwire 5620 RTU Installation Instructions

[Go to Top](#)

POTS Filters and Splitters

5030-A2-GN10-20 12/99

Hotwire 5030 POTS Splitter Customer Premises Installation Instructions

5038-A2-GN10-10 9/98

Hotwire 5038 Distributed POTS Splitter Customer Premises Installation Instructions

EXHIBIT A

5038-A2-GN11-10 4/98
Hotwire 5038 MVL POTS Filter Customer Premises Installation Instructions
Hotwire 6035 Universal Phone Filter Installation Instructions

6038-A2-GN10-00 6/98
Hotwire 6038 MVL POTS Filter Customer Premises Installation Instructions

6040-A2-GN11-00 12/99
Hotwire 6040 MVL Wall Jack Phone Filter Installation Instructions

7034-A2-GN10-00 4/00
Hotwire 7034 Customer Premises POTS Splitter Installation Instructions

[Go to Top](#)

If you are looking for older versions of bridge and router technical manuals, [click here](#).

Copyright 1996 - 2005 Paradyne Corporation
8545 - 126th Avenue North . Largo, Florida, USA 33773
Worldwide: **1-727-530-2000** . Fax: 1-727-530-8216
[Contact Us](#)

EXHIBIT A

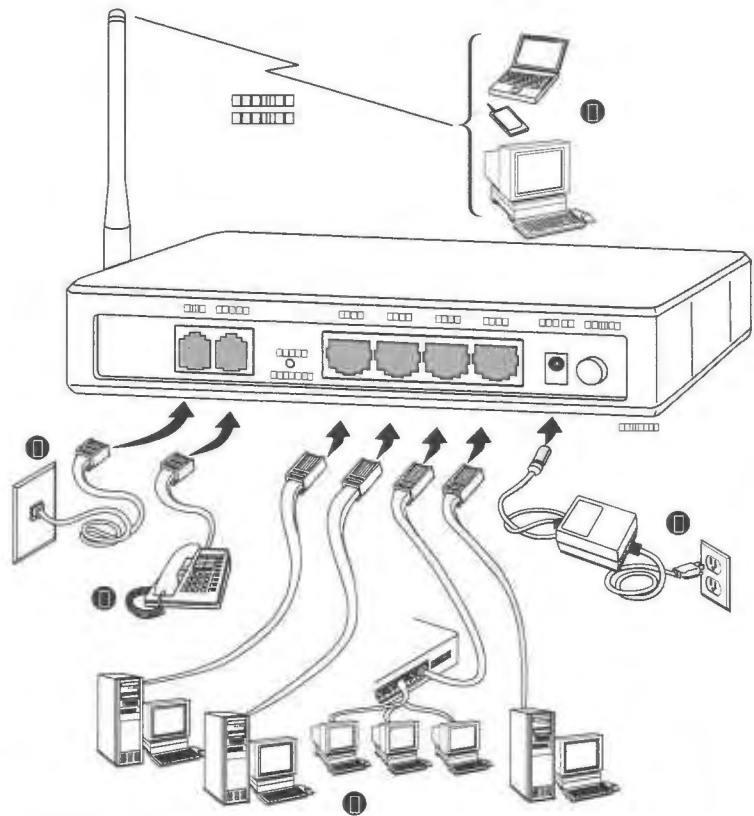
<http://web.archive.org/web/20060106200402/http://www.paradyne.com/support/manuals/docs/6388-A2-GZ10-00.pdf>

6388 Wireless Router
Quick Installation Instructions
Document Number 6388-A2-GZ10-00
February 2005

Installation

- 1 Connect the DSL line to the LINE jack using the provided RJ11 cable.
- 2 Optionally, connect a phone to the PHONE jack. This phone does not require a POTS splitter.
- 3 Connect PCs, hubs, and switches to the LAN ports. Either a straight-through Ethernet cable (provided) or a crossover cable can be used. The router automatically determines the type of signal required.
- 4 Attach the power adapter. The supplied power adapter may look different than the one illustrated here.
- 5 Configure your router and your wireless devices to communicate with each other.

See the user's guide on the CD for information about configuring your router using your web browser.



* 6388- A2- GZ10- 00*
6388-A2-GZ10-00

Copyright © 2005 Paradyne Corporation.

Software and Firmware License Agreement

ONCE YOU HAVE READ THIS LICENSE AGREEMENT AND AGREE TO ITS TERMS, YOU MAY USE THE SOFTWARE AND/OR FIRMWARE INCORPORATED INTO THE PARADYNE PRODUCT. BY USING THE PARADYNE PRODUCT YOU SHOW YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE AGREEMENT.

IN THE EVENT THAT YOU DO NOT AGREE WITH ANY OF THE TERMS OF THIS LICENSE AGREEMENT, PROMPTLY RETURN THE UNUSED PRODUCT IN ITS ORIGINAL PACKAGING AND YOUR SALES RECEIPT OR INVOICE TO THE LOCATION WHERE YOU OBTAINED THE PARADYNE PRODUCT OR THE LOCATION FROM WHICH IT WAS SHIPPED TO YOU, AS APPLICABLE, AND YOU WILL RECEIVE A REFUND OR CREDIT FOR THE PARADYNE PRODUCT PURCHASED BY YOU.

The terms and conditions of this License Agreement (the "Agreement") will apply to the software and/or firmware (individually or collectively the "Software") incorporated into the Paradyne product (the "Product") purchased by you and any derivatives obtained from the Software, including any copy of either. If you have executed a separate written agreement covering the Software supplied to you under this purchase, such separate written agreement shall govern.

Paradyne Corporation ("Paradyne") grants to you, and you ("Licensee") agree to accept a personal, non-transferable, non-exclusive, right (without the right to sublicense) to use the Software, solely as it is intended and solely as incorporated in the Product purchased from Paradyne or its authorized distributor or reseller under the following terms and conditions:

1. Ownership: The Software is the sole property of Paradyne and/or its licensors. The Licensee acquires no title, right or interest in the Software other than the license granted under this Agreement.
2. Licensee shall not use the Software in any country other than the country in which the Product was rightfully purchased except upon prior written notice to Paradyne and an agreement in writing to additional terms.
3. The Licensee shall not reverse engineer, decompile or disassemble the Software in whole or in part.
4. The Licensee shall not copy the Software except for a single archival copy.

EXHIBIT A

5. Except for the Product warranty contained in the Product, the Software is provided "AS IS" and in its present state and condition and Paradyne makes no other warranty whatsoever with respect to the Product purchased by you. THIS AGREEMENT EXPRESSLY EXCLUDES ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, OR ORAL OR WRITTEN, INCLUDING WITHOUT LIMITATION:

- a. Any warranty that the Software is error-free, will operate uninterrupted in your operating environment, or is compatible with any equipment or software configurations; and
- b. ANY AND ALL IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

Some states or other jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty lasts, so the above limitations may not apply to you. This warranty gives you specific legal rights, and you may also have other rights which vary from one state or jurisdiction to another.

6. In no event will Paradyne be liable to Licensee for any consequential, incidental, punitive or special damages, including any lost profits or lost savings, loss of business information or business interruption or other pecuniary loss arising out of the use or inability to use the Software, whether based on contract, tort, warranty or other legal or equitable grounds, even if Paradyne has been advised of the possibility of such damages, or for any claim by any third party.
7. The rights granted under this Agreement may not be assigned, sublicensed or otherwise transferred by the Licensee to any third party without the prior written consent of Paradyne.
8. This Agreement and the license granted under this Agreement shall be terminated in the event of breach by the Licensee of any provisions of this Agreement.
9. Upon such termination, the Licensee shall refrain from any further use of the Software and destroy the original and all copies of the Software in the possession of Licensee together with all documentation and related materials.
10. This Agreement shall be governed by the laws of the State of Florida, without regard to its provisions concerning conflicts of laws.

EXHIBIT A

<https://web.archive.org/web/20060106201139/http://www.paradyne.com/support/manuals/docs/6388-A2-GB20-00.pdf>

6388 Wireless Router

User's Guide

Document No. 6388-A2-GB20-00

February 2005



Copyright © 2005 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- Internet: Visit the Paradyne World Wide Web site at www.paradyne.com. (Be sure to register your warranty at www.paradyne.com/warranty.)
- Telephone: Call our automated system to receive current information by fax or to speak with a company representative.
 - Within the U.S.A., call 1-800-870-2221
 - Outside the U.S.A., call 1-727-530-2340

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to userdoc@paradyne.com. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Trademarks

Acculink, Bitstorm, Comsphere, DSL the Easy Way, ETC, Etherloop, FrameSaver, GrandSLAM, GrandVIEW, Hotwire, the Hotwire logo, iMarc, Jetstream, MVL, NextEDGE, Net to Net Technologies, OpenLane, Paradyne, the Paradyne logo, Paradyne Credit Corp., the Paradyne Credit Corp. logo, Performance Wizard, ReachDSL, StormPort, TruePut are registered trademarks of Paradyne Corporation.

ADSL/R, Connect to Success, Hotwire Connected, JetFusion, JetVision, MicroBurst, PacketSurfer, Quick Channel, Reverse Gateway, Spectrum Manager, and StormTracker are trademarks of Paradyne Corporation.

All other products or services mentioned herein are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

▲ Important Safety Instructions

1. Read and follow all warning notices and instructions marked on the product or included in the manual.
2. Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.
3. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.
4. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
5. General purpose cables are used with this product for connection to the network. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer. Use a UL Listed, CSA certified, minimum No. 24 AWG line cord for connection to the Digital Subscriber Line (DSL) network.
6. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
7. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are interconnected, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.
8. Input power to this product must be provided by one of the following: (1) a UL Listed/CSA certified power source with a Class 2 or Limited Power Source (LPS) output for use in North America, or (2) a certified transformer, with a Safety Extra Low Voltage (SELV) output having a maximum of 240 VA available, for use in the country of installation.
9. In addition, since the equipment is to be used with telecommunications circuits, take the following precautions:
 - Never install telephone wiring during a lightning storm.
 - Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
 - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
 - Use caution when installing or modifying telephone lines.
 - Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
 - Do not use the telephone to report a gas leak in the vicinity of the leak.

CE Marking

When the product is marked with the CE mark on the equipment label, a supporting Declaration of Conformity may be downloaded from the Paradyne World Wide Web site at www.paradyne.com. Select Library → Technical Manuals → CE Declarations of Conformity.

FCC Part 15 Declaration

An FCC Declaration of Conformity may be downloaded from the Paradyne World Wide Web site at www.paradyne.com. Select Support -> Technical Manuals -> Declarations of Conformity.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by the responsible party.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice to Users of the United States Telephone Network

The following notice applies to versions of the modem that have been FCC Part 68 approved.

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council for Terminal Attachment (ACTA). On the bottom side of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the Telephone Company.

This equipment is intended to connect to the Public Switched Telephone Network through a Universal Service Order Code (USOC) type RJ11C jack. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It has been designed to be connected to a compatible modular jack that is also compliant.

The Ringer Equivalence Number (or REN) is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local Telephone Company. The REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point. For example, 03 represents a REN of 0.3.

If the modem causes harm to the telephone network, the Telephone Company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the Telephone Company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The Telephone Company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the Telephone Company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. If trouble is experienced with the modem, refer to the repair and warranty information in this document.

If the equipment is causing harm to the telephone network, the Telephone Company may request that you disconnect the equipment until the problem is resolved.

The user may make no repairs to the equipment.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

If the site has specially wired alarm equipment connected to the telephone line, ensure the installation of the modem does not disable the alarm equipment. If you have questions about what will disable alarm equipment, consult your Telephone Company or a qualified installer.

Supplier's Declaration of Conformity

Place of Issue:

Paradyne Corporation
8545 126th Avenue North
Largo, FL 33773-1502
USA

Date of Issue: TBD

Paradyne Corporation, located at the above address, hereby certifies that the Model Number 6388-AX-XXX (where X may be any numeric character) bearing labeling identification number US:AW2DL04B6388-AX complies with: the Federal Communications Commission's ("FCC") Rules and Regulations 47 CFR Part 68, the Administrative Council on Terminal Attachments ("ACTA")-adopted technical criteria TIA-968-A, "Telecommunications - Telephone Terminal Equipment -Technical Requirements for Connection of Terminal Equipment To the Telephone Network, October 2002."

Patrick Murphy

Senior Vice President, Chief Financial Officer



Notice to Users of the Canadian Telephone Network

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation IC before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is labeled on the equipment. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

If your equipment is in need of repair, contact your local sales representative, service representative, or distributor directly.

 CANADA - EMI NOTICE:

This Class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du règlement sur le matériel brouilleur du Canada.

Japan Notices

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Contents

About This Guide

- Document Purpose and Intended Audience v
- Document Summary v
- Product-Related Documents v

1 Introduction

- Definitions 1-1
- Features of the 6388 Wireless Router 1-1
- System Requirements 1-2
- Ports and Buttons (Back Panel) 1-2
- LED Description (Front Panel) 1-2
- Packing List 1-3

2 Hardware Installation and PC Setup

- Overview 2-1
- Connecting the Hardware 2-1
- Configuring Your PC's IP Address 2-3
 - Assigning an IP Address to your PC Automatically by DHCP 2-3
 - Windows XP 2-3
 - Windows 2000 2-5
 - Windows ME 2-6
 - Windows 95, 98 2-7
 - Windows NT 4.0 2-8

3 Using the Web Interface

- Logging Into Your Router 3-1
- Home Page 3-2
- Quick Start 3-2
- Setup 3-5
 - Wide Area Network Connection 3-5
 - Local Area Network Connection 3-5
 - Saving Changes 3-5
- Configuring the WAN 3-6

□ New Connection	3-7
PPPoE Connection Setup	3-7
PPPoA Connection Setup	3-9
Static Connection Setup	3-11
DHCP Connection Setup	3-12
Bridged Connection	3-14
CLIP Connection	3-15
□ Modify an Existing Connection	3-16
□ Modem Setup	3-17
□ TSML	3-18
□ Configuring the LAN	3-19
Enable/Disable DHCP	3-19
□ Changing the Router's IP address	3-20
□ Ethernet Switch	3-21
□ Firewall/NAT Services	3-22
□ Advanced	3-23
UPnP	3-23
SNTP	3-24
SNMP	3-25
IP QoS	3-26
Port Forwarding	3-26
IP Filters	3-28
LAN Clients	3-29
VLAN	3-29
Bridge Filters	3-30
Web Filters	3-32
Multicast	3-33
IGMP Snooping	3-34
Static Routing	3-34
Dynamic Routing	3-35
Access Control	3-37
Log Out	3-37
□ Wireless	3-38
Setup	3-38
Configuration	3-40
Security	3-40
Management	3-43

□ Tools	3-45
System Commands	3-45
Remote Log	3-45
User Management	3-47
Update Gateway	3-48
□ Analyzer	3-49
Ping Test	3-50
Modem Test	3-51
□ Status	3-52

4 Troubleshooting

□ The Router Is Not Functional	4-1
□ You Cannot Connect to the Router	4-1
□ LEDs Blink in a Sequential Pattern	4-2
□ Status LED Continues to Blink	4-2
□ Status LED is Always Off	4-2

A Terminology

□ What is a Firewall?	A-1
□ What is NAT?	A-1
□ What is a DMZ?	A-1
□ What is a Router?	A-2

Index

About This Guide

Document Purpose and Intended Audience

This guide contains detailed information about the 6388 wireless router. It is intended for all users of the router.

Document Summary

Section	Description
Chapter 1, Introduction	Describes the features of the router.
Chapter 2, Hardware Installation and PC Setup	Shows how to connect the router and set up your PC to manage the router.
Chapter 3, Using the Web Interface	Explains how to use the web interface to configure and monitor the router.
Chapter 4, Troubleshooting	Contains tips on troubleshooting common problems.
Appendix A, Terminology	Explains some major internetworking concepts.
Index	Lists key terms, concepts, and sections in alphabetical order.

A master glossary of terms and acronyms used in Paradyne documents is available online at www.paradyne.com. Select Support → Technical Manuals → [Technical Glossary](#).

Product-Related Documents

Complete documentation for Paradyne products is available online at www.paradyne.com. Select Support → Technical Manuals.

To order a paper copy of a Paradyne document, or to speak with a sales representative, please call 1-727-530-2000.

Introduction

1

Definitions

Before you install or use your new router, you may find it helpful to understand the following terms:

- A bridge is a device that forwards any message from one part of a network to another.
- A router is a device that forwards messages according to their network addresses.
- ADSL is Asymmetric Digital Subscriber Line, a version of DSL that allows a higher speed for information coming from the Internet to your PC ("downstream") than it does for information going to the Internet from your PC ("upstream").
- ReachDSL[®] is a version of DSL that works on lines too long or too noisy for ADSL.
- ADSL/R[®] is technology that combines ADSL and ReachDSL in one device.

The Model 6388 is a Digital Subscriber Line (DSL) modem that may be set by you to run in bridge or router mode. Because it is most frequently used as a router, that is how it is referred to in this manual. It supports ADSL/R.

Features of the 6388 Wireless Router

Your router has the following features:

- 4-Port 10/100BaseT Layer 2 Ethernet switch
- Support for ADSL2+ and ReachDSL (ADSL/R)
- Support for wireless protocols 802.11b and 802.11g
- The ability to connect multiple PCs to the Internet with just one WAN IP Address (when configured in router mode with NAT enabled)
- A user-friendly web interface for configuration and monitoring
- Single-session IPsec and PPTP passthrough for Virtual Private Network (VPN)

- Preconfigured port settings for many popular games
- Ability to act as a DHCP Server on your network
- Compatibility with virtually all standard Internet applications
- Address filtering and DMZ hosting
- Downloadable flash software upgrades
- Support for up to eight Permanent Virtual Circuits (PVCs)
- Support for up to eight PPPoE sessions

System Requirements

In order to use your modem for Internet access, you must have the following:

- ADSL service subscription from your ISP.
- One computer with an Ethernet 10/100BaseT network interface card (NIC).
- For system monitoring or configuration using the supplied web interface, a web browser such as Internet Explorer Version 5.5 or later.

Ports and Buttons (Back Panel)

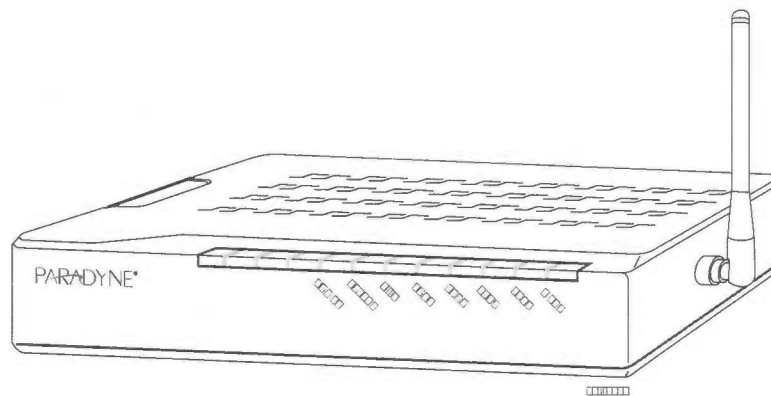
- LINE port: This is the DSL interface which connects directly to your phone line.
- PHONE port: This allows a phone to directly connect to the router. You do not need to add splitter to the phone you connect here, since the router has an internal splitter.
- RESET Button: The RESET button is used to reset the router to the default settings selected by your service provider. Do not use the RESET button unless advised to by your service representative.
- LAN 1–4 (Local Area Network) port(s): connect to Ethernet network devices, such as a PC, hub, switch, or router. Depending on the device connected, you may need a crossover cable or a straight-through cable.
- POWER is where you connect the power supply.
- ON/OFF: Controls power to the router. The router is on when this button is in its down position, and off when the button is in its up position.

LED Description (Front Panel)

- Power LED: On indicates that the power is supplied to the router.
- Status LED: The Status LED serves two purposes. If the LED is continuously lit, the DSL interface is successfully connected to a device through the LINE

port. If the LED is flickering, it is an indication that the router is training (negotiating the connection to its partner modem).

- Link LED: The Activity LED shows the state of the PPPoA or PPPoE connection. Off: no PPP connection is established or the connection is not used. Blinking: a PPP connection is being attempted. Solid green: a PPP connection is established. Flickering: a PPP connection is established and there is activity on the link.
- LAN 1–4 LED: Each LAN LED serves two purposes. If the LED is continuously lit, the Ethernet interface is successfully connected to a device through the LAN port. If the LED is flickering, it is an indication of network activity.
- WLAN: Solid green: the wireless LAN is enabled. Flickering: there is activity on the wireless LAN.



Packing List

- Your router is shipped with the following:
- Power adapter
- Ethernet cable (RJ45, straight-through wiring)
- Phone cable (RJ11)
- CD-ROM containing this manual

Hardware Installation and PC Setup

2

Overview

This chapter provides basic instructions for connecting the router to a computer or a LAN and to the Internet using DSL. The first part provides instructions to set up the hardware, and the second part describes how to prepare your PC for use with the router. Refer to Chapter 3, Using the Web Interface for router configuration instructions.

It is assumed that you have already subscribed to DSL service with your Internet service provider (ISP).

Connecting the Hardware

Shut down your PC and any other equipment before connecting it to the router. To connect your router:

► Procedure

1. Connect the supplied modular phone cable to the LINE port, and connect the other end of the cable to your phone jack.
2. If you would like to use a phone in the vicinity of the router, connect it to the PHONE jack of the router using the cord that came with your telephone. The router has an internal POTS filter, so you do not need to install one here.
3. Use the included Ethernet cable to connect your computer to the router. Attach one end of the Ethernet cable to one of the LAN ports on the back of the router and connect the other end to the Ethernet port or Network Interface Card (NIC) in your PC.

Connect any other PCs, hubs, and switches to the remaining LAN ports. Either a crossover or a straight-through Ethernet cable can be used: the router determines and adjusts to the type of signal required.

4. Connect the cylindrical power plug into the POWER connector on the back of the device. Next:
 - If you have a wall-mount adapter, plug the AC adapter into a wall outlet or a power strip.

- If you have a table-top adapter, use the AC power cord to connect the adapter to a wall outlet or power strip.

The supplied power adapter may look different than the one illustrated here.

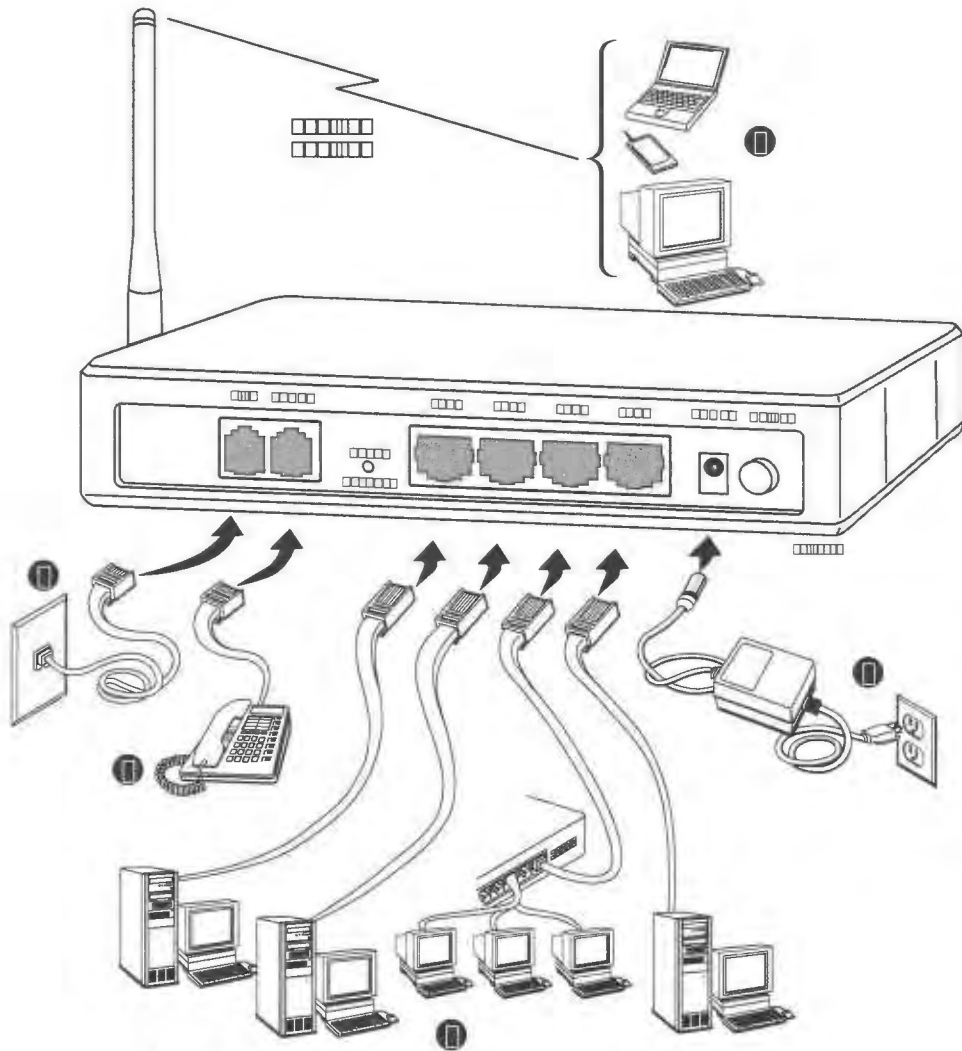


Figure 2-1. Hardware Installation

5. Configure your router and your wireless devices to communicate with each other.
6. Turn on your PC any other LAN devices, such as hubs or switches.

Configuring Your PC's IP Address

Before you start to access the router using the Ethernet connection, you must configure your PC to use DHCP, or change your PC's TCP/IP address to be 192.168.1.x, where x is any number between 2 and 254, with a subnet mask of 255.255.255.0.

Your router's default IP address is 192.168.1.1.

Assigning an IP Address to your PC Automatically by DHCP

To use the router's DHCP feature, click in the radio button labeled "Obtain an IP address automatically" instead of "Use the following IP address" in the following procedures.

By default, the LAN port IP address of the router is 192.168.1.1. (You can change this address, or another address can be assigned by your ISP.)

Windows XP

To configure the IP address under Windows XP:

► Procedure

1. In the Windows task bar, click on the Start button, and then click on Control Panel.
2. Double-click on the Network Connections icon.
3. In the LAN or High-Speed Internet window, right-click on the icon corresponding to your network interface card (NIC) and select Properties. (Often this icon is labeled Local Area Connection). The Local Area Connection dialog box is displayed with a list of currently installed network items.

4. Ensure that the check box to the left of the item labeled Internet Protocol (TCP/IP) is checked, and click on Properties.

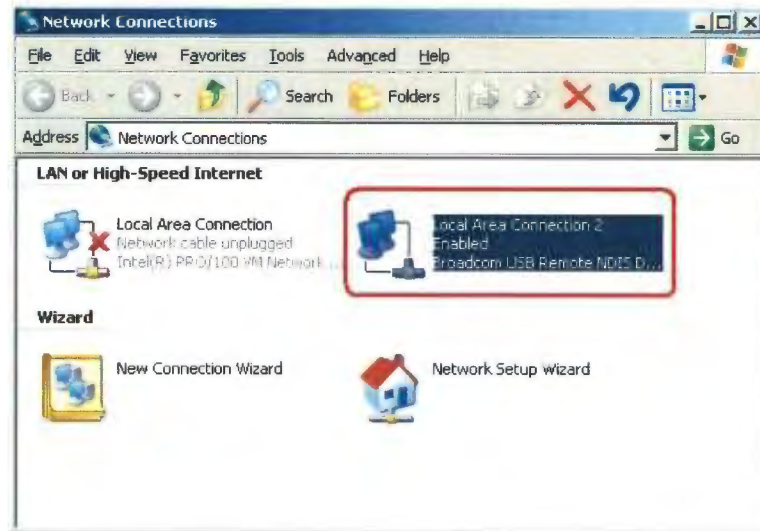


Figure 2-2. Network Connections in Windows XP

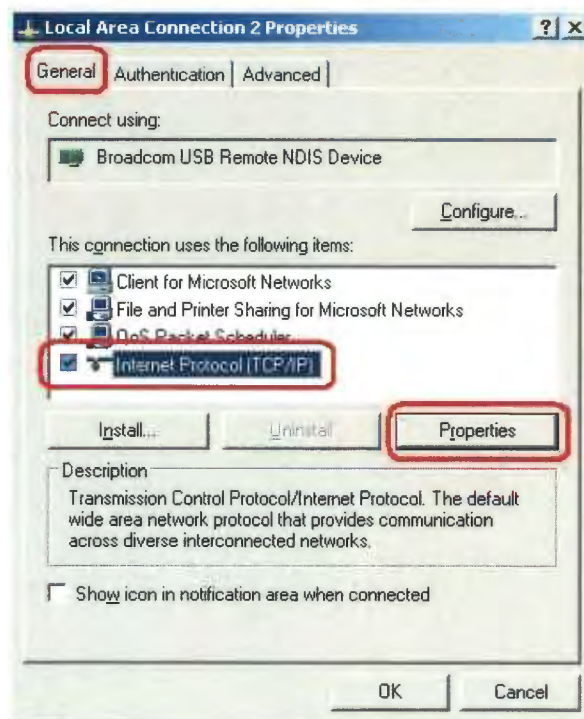


Figure 2-3. Local Area Connection Properties in Windows XP

5. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled "Use the following IP address" and type 192.168.1.x (where x is any number between 2 and 254) in the IP Address field. Type 255.255.255.0 in the Subnet Mask field.

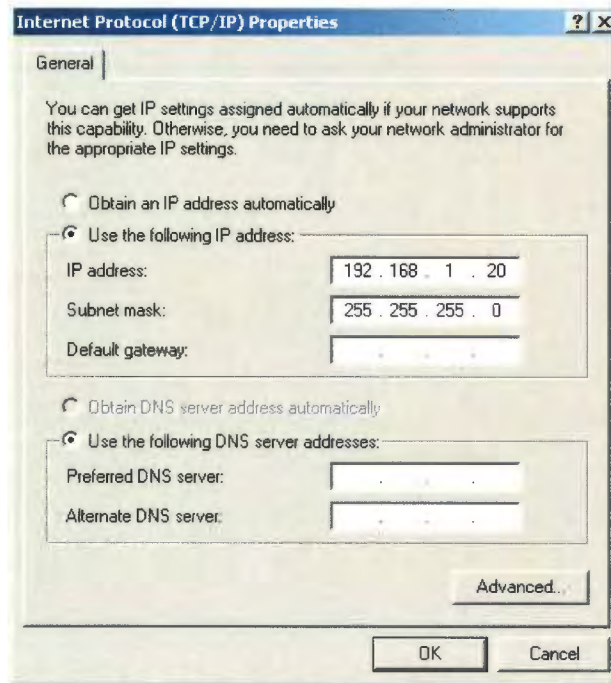


Figure 2-4. TCP/IP Properties in Windows XP

6. Click on OK twice to confirm your changes, and close the Control Panel.

Windows 2000

To configure the IP address under Windows 2000:

► Procedure

1. In the Windows task bar, click on the Start button, point to Settings, and then select Control Panel.
2. Double-click on the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click on the Local Area Connection icon, and then select Properties.

The Local Area Connection Properties dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), the protocol has already been enabled, in which case you can skip to Step 10.

4. If Internet Protocol (TCP/IP) does not appear as an installed component, click on Install.
5. In the Select Network Component Type dialog box, select Protocol, and then click on Add.
6. Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click on OK.

You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
7. If prompted, click on OK to restart your computer with the new settings.
8. After restarting your PC, double-click on the Network and Dial-up Connections icon in the Control Panel.
9. In Network and Dial-up Connections window, right-click on the Local Area Connection icon, and then select Properties.
10. In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP), and then click on Properties.
11. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled "Use the following IP address" and type 192.168.1.x (where x is any number between 2 and 254) in the IP Address field. Type 255.255.255.0 in the Subnet Mask field.
12. Click on OK twice to confirm and save your changes, and then close the Control Panel.

Windows ME

To configure the IP address under Windows ME:

► Procedure

1. In the Windows task bar, click on the Start button, point to Settings, and then click on Control Panel.
2. Double-click on the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click on the Network icon, and then select Properties.

The Network Properties dialog box is displayed with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), the protocol has already been enabled, in which case you can skip to Step 11.

4. If Internet Protocol (TCP/IP) does not appear as an installed component, click on Add.
5. In the Select Network Component Type dialog box, select Protocol, and then click on Add.
6. Select Microsoft in the Manufacturers box.
7. Select Internet Protocol (TCP/IP) in the Network Protocols list, and then click on OK.

You may be prompted to install files from your Windows ME installation CD or other media. Follow the instructions to install the files.

8. If prompted, click on OK to restart your computer with the new settings.
9. After restarting your PC, double-click on the Network and Dial-up Connections icon in the Control Panel.
10. In Network and Dial-up Connections window, right-click on the Network icon, and then select Properties.
11. In the Network Properties dialog box, select TCP/IP, and then click on Properties.
12. In the TCP/IP Settings dialog box, click in the radio button labeled "Use the following IP address" and type 192.168.1.x (where x is any number between 2 and 254) in the IP Address field. Type 255.255.255.0 in the Subnet Mask field.
13. Click on OK twice to confirm and save your changes, and then close the Control Panel.

Windows 95, 98

To configure the IP address under Windows 95 or Windows 98:

► Procedure

1. In the Windows task bar, click on the Start button, point to Settings, and then click on Control Panel.
2. Double-click on the Network icon.

The Network dialog box is displayed with a list of currently installed network components. If the list includes TCP/IP, the protocol has already been enabled, in which case you can skip to Step 9.
3. If TCP/IP does not appear as an installed component, click on Add. The Select Network Component Type dialog box appears.
4. Select Protocol, and then click on Add. The Select Network Protocol dialog box appears.
5. Click on Microsoft in the Manufacturers list box, and then click on TCP/IP in the Network Protocols list box.
6. Click on OK to return to the Network dialog box, and then click on OK again.

You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.

7. Click on OK to restart the PC and complete the TCP/IP installation.
8. After restarting your PC, open the Control Panel window, and then click on the Network icon.
9. Select the network component labeled TCP/IP, and then click on Properties.

If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.

10. In the TCP/IP Properties dialog box, click on the IP Address tab.
11. Click in the radio button labeled "Use the following IP address" and type 192.168.1.x (where x is any number between 2 and 254) in the IP Address field. Type 255.255.255.0 in the Subnet Mask field.
12. Click on OK twice to confirm and save your changes. You will be prompted to restart Windows. Click on Yes and restart your PC again.

Windows NT 4.0

To configure the IP address under Windows NT 4.0:

► Procedure

1. In the Windows NT task bar, click on the Start button, point to Settings, and then click on Control Panel.
2. In the Control Panel window, double click on the Network icon.
3. In the Network dialog box, click on the Protocols tab.

The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP, the protocol has already been enabled, in which case you can skip to Step 9.

4. If TCP/IP does not appear as an installed component, click on Add.
5. In the Select Network Protocol dialog box, select TCP/IP, and then click on OK.

You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.

After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.

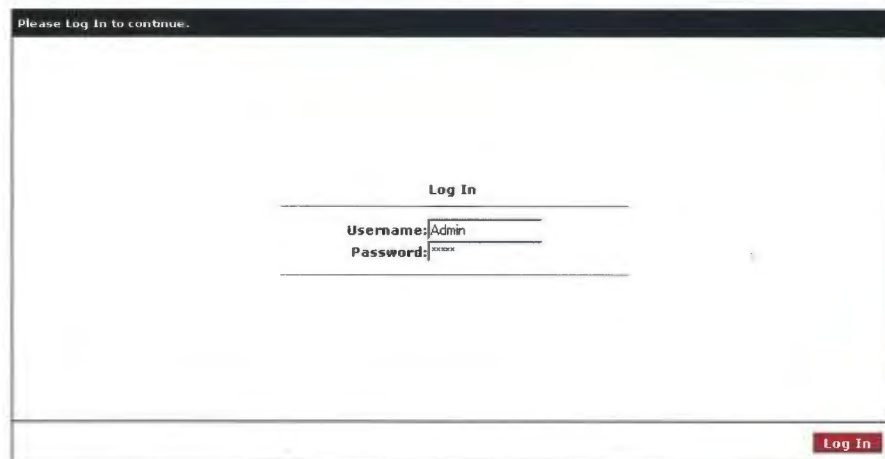
6. Click on Yes to continue, and then click on OK if prompted to restart your computer.
7. After restarting your PC, open the Control Panel window, and then double-click on the Network icon.
8. In the Network dialog box, click on the Protocols tab.
9. In the Protocols tab, select TCP/IP, and then click on Properties.
10. In the Microsoft TCP/IP Properties dialog box, click in the radio button labeled Use the following IP address and type 192.168.1.x (where x is any number between 2 and 254) in the IP Address field. Type 255.255.255.0 in the Subnet Mask field.
11. Click on OK twice to confirm and save your changes, and then close the Control Panel.

Using the Web Interface

3

Logging Into Your Router

To configure your router, open your web browser. Ignore any error about lacking a connection. Type the default IP address (192.168.1.1) into the Location field of your browser and press the Enter key. The following screen appears.



Please Log In to continue.

Log In

Username: Admin

Password: xxxxx

Log In

Figure 3-1. Login Screen

The default user name is Admin and the password is Admin. Both are case-sensitive.

Note: Before configuring your router, make sure you have followed the instructions in [Chapter 2, Hardware Installation and PC Setup](#). You should have your PCs configured for DHCP mode (if your router will be), and have proxies disabled on your browser. If you see a login redirection screen when you access the web interface, verify that JavaScript support is enabled in your browser. Also, if you do not get the screen shown in [Figure 3-1](#), you may need to delete your temporary Internet files.

Home Page

The first screen (Figure 3-2) that appears after the log in screen is the Home page. From this screen you can configure the LAN and WAN connections, configure the router's security, routing, and filtering, access debugging tools, obtain the status of the router, and view the online help.

Description	Type	IP	State	Online	Disconnect Reason
TSML	tsml	NA	NA	NA	NA
QK_CONN	dhcpc	135.26.11.220	Connected	0hr 5min 51sec	NA

Figure 3-2. Home Page

The basic layout of the Home page consists of a page selection list across the top of the browser window. The footer displays router status, connection information, and other useful information. The center display is where most of the configuration will take place.

Click on Log Out to close the session, Refresh to update the status display, or Quick Start to configure basic options.

Quick Start

The Quick Start screen gives you immediate access to the options you are most likely to need to specify or change. Click on the Quick Start button on the Home page to access it.

Select a connection type from the drop-down list:

- DHCP – The address of the router is automatically assigned
- PPPoE – Your service provider has restricted access by name and password
- Static – Your service provider has supplied a specific network address for your router



Figure 3-3. Quick Start - DHCP

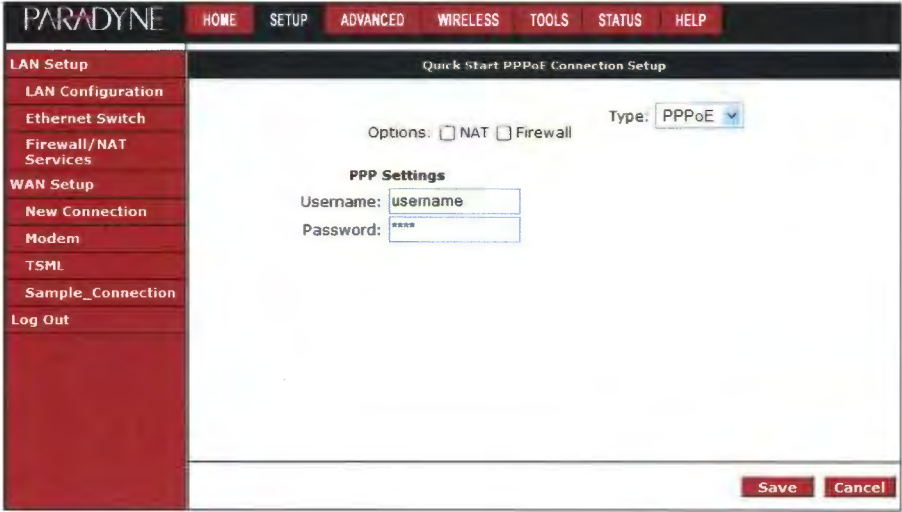


Figure 3-4. Quick Start - PPPoE

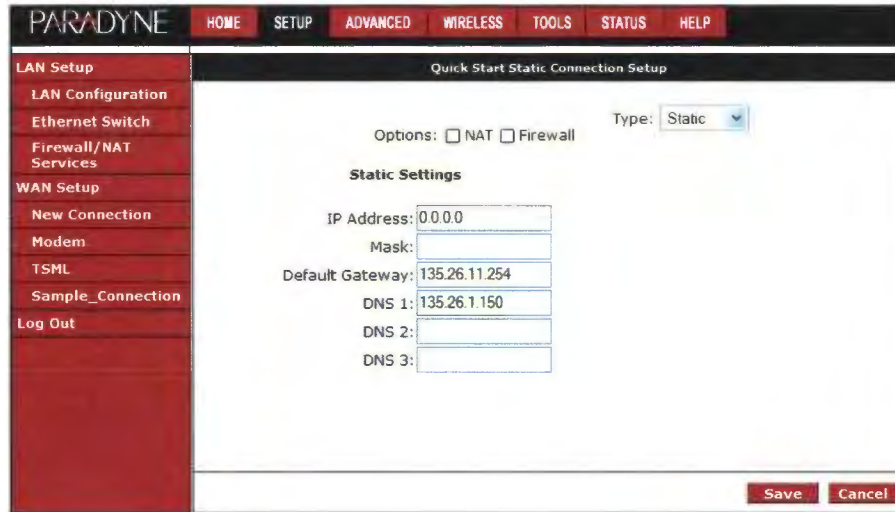


Figure 3-5. Quick Start - Static

Enter or select Quick Start options as shown in the following table.

Table 3-1. Quick Start Options

Field	Description
NAT	Click in the check box to activate Network Address Translation (NAT). See Appendix A, Terminology , for a description of NAT.
Firewall	Click in the check box to activate the firewall. See Appendix A, Terminology , for a description of a firewall.
Username (PPPoE)	Enter the user name given to you by your service provider.
Password (PPPoE)	Enter the password given to you by your service provider.
IP Address (Static)	Enter the IP address to be assigned to the router.
Mask (Static)	Enter the subnet mask to be applied to the IP address.
Default Gateway (Static)	Enter the IP address of a default gateway. Packets for which the router has no appropriate route are sent to the default gateway.
DNS 1–3 (Static)	Enter the IP address of the primary domain name server, and optionally the addresses of a secondary and tertiary DNS to be used if the server before it is unavailable.

Click on Save to make the changes permanent.

Setup

To set up LAN and WAN options not available on the Quick Start screens, select Setup from the Home page. Figure 3-6 shows the Setup page. The menu is broken into two sections: the WAN configuration and the LAN configuration.

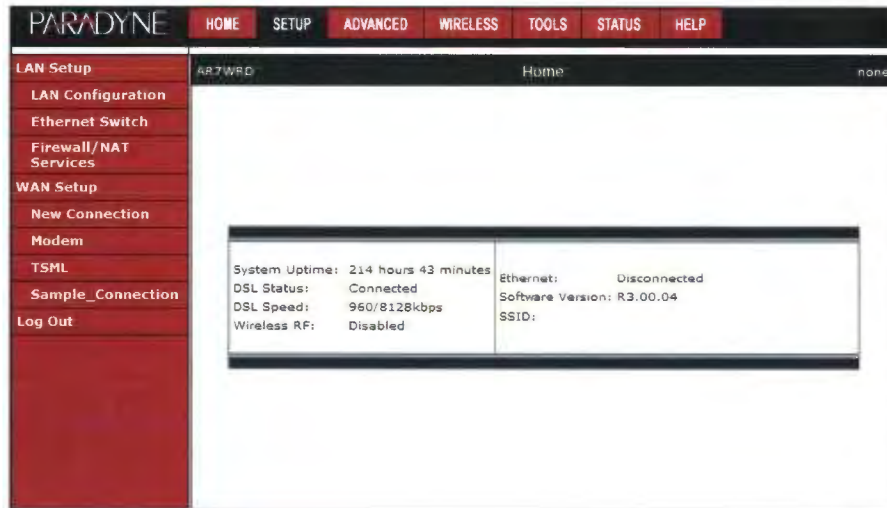


Figure 3-6. Setup Options

Wide Area Network Connection

The DSL (LINE) connection is the Wide Area Network (WAN) connection. It is also referred to as a broadband connection. The requirements for the WAN connection depend on your Internet Service Provider (ISP). Most of the configuration you will perform will be in this area.

Local Area Network Connection

On the other side of your router are your own Local Area Network (LAN) connections. This is where you plug in your local computers to the router. The router is normally configured to automatically provide all the PCs on your network with Internet addresses.

If you connected a PC (rather than a hub or a switch) directly to the router, your LAN consists of that PC.

Saving Changes

Note that the Apply button temporarily saves changes you make. To make changes permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Configuring the WAN

Before the router will pass any data between the LAN interface and the WAN interface, the WAN side of the router must be configured. Depending upon your ISP, you will need some or all of the information listed below before you can properly configure the WAN:

- Your DSL line's Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI)
- Your DSL encapsulation type and multiplexing mode
- Your DSL training mode (default is MMODE)

If you use PPPoA or PPPoE, you also need these values from your ISP:

- Your username and password

If you use multiprotocol encapsulation over ATM Adaptation Layer 5 (as described in RFC 1483), you may need these values from your ISP:

- Your DSL fixed Internet IP address
- Your subnet mask
- Your default gateway IP address
- Your primary DNS IP address

Since multiple users can use the router, the router can simultaneously support multiple connection types. You must set up different profiles for each connection. The router supports the following protocols:

- DHCP
- PPPoA (RFC 2364)
- PPPoE (RFC 2516)
- Static
- Bridged

New Connection

A new connection is basically a virtual connection. Your router can support up to 8 different virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the router to pass data correctly.

PPPoE Connection Setup

PPPoE is defined in the Internet standard RFC 2516. It is a method of encapsulating PPP packets over Ethernet. PPP (Point-to-Point Protocol) is a method of establishing a network session between network hosts. It usually provides a mechanism of authenticating users.

To configure the CPE for PPPoE:

► Procedure

1. Click on Setup and then click on New Connection. The default PPPoE connection setup is displayed.
2. At the Type field, select PPPoE from the drop-down list. The PPPoE Connection Setup page is displayed.
3. Give your PPPoE connection a unique name. The name must not have spaces and cannot begin with numbers.
4. Select a PVC Sharing type of Disable, Enable, or VLAN.
5. Select or enter a VPI and VCI (as supplied by your DSL service provider or your ISP), or click in Auto PVC. (Auto PVC causes the router to perform automatic VPI/VCI detection as defined in DSL forum TR-068.) For VLAN, specify a VLAN ID and priority.
6. Select NAT and Firewall if you want them active for this connection. Firewall and NAT services must be enabled. See Firewall/NAT Services on page 3-22.
7. Select the quality of service (QoS). Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:
 - PCR (Peak Cell Rate)
 - SCR (Sustainable Cell Rate)
 - MBS (Maximum Burst Size)
 - CDVT (Cell Delay Variation Tolerance)

Following is a description of the different options:

- Username - The username for the PPPoE access. This is provided by your DSL service provider or your ISP.
- Password - The password for the PPPoE access. This is provided by your DSL service provider or your ISP.

- Idle Timeout - Specifies that PPPoE connection should disconnect if the link has no activity detected for the specified number of seconds. This field is used in conjunction with the On Demand feature. To disable the timeout feature, enter a zero in this field.
- Authentication – Specifies the authentication protocol: Auto (the protocol is selected by the PPPoE server), PAP (Password Authentication Protocol), or CHAP (Challenge Handshake Authentication Protocol).
- Keep Alive - When the On Demand option is not enabled, this value specifies the length of time to keep the connection from being shut down for inactivity by sending PPP LCP echoes to the PPP server. To ensure that the link is always active, enter a zero in this field.
- MTU - The Maximum Transmission Unit the DSL connection can send. It is a negotiated value. The maximum specified value is 1500, although some DSL/ISP providers require a larger value. The minimum MTU value is 128.
- On Demand - Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
- Default Gateway – Specifies whether a default gateway is used.
- Enforce MTU - Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MTU by changing TCP Maximum Segment Size to the PPP MTU.
- Debug - Enables PPPoE connection debugging facilities. Debugging is talked about later.
- PPP Unnumbered – Specifies that the calling and answering routers will not request IP addresses.

The screenshot shows the Paradyne web interface for PPPoE Connection Setup. The navigation menu on the left includes LAN Setup, WAN Setup, and New Connection. The main configuration area is titled 'PPPoE Connection Setup' and contains the following fields and options:

- Name: [text input]
- Type: PPPoE (dropdown)
- Sharing: Disable (dropdown)
- Options: NAT Firewall
- VLAN ID: [text input]
- Priority Bits: [text input]
- PPP Settings:
 - Username: username
 - Password: [password input]
 - Idle Timeout: [text input] secs
 - Keep Alive: 1 min
 - Authentication: Auto CHAP PAP
 - MTU: 1492 bytes
 - On Demand:
 - Enforce MTU:
 - PPP Unnumbered:
- PVC Settings:
 - PVC: [text input]
 - VPI: 0
 - VCI: 0
 - QoS: UBR (dropdown)
 - PCR: [text input] cps
 - SCR: [text input] cps
 - MBS: [text input] cells
 - CDVT: [text input] usecs
 - Auto PVC:
- Default Gateway:
- Debug:
- Buttons: Connect, Disconnect, Apply, Delete, Cancel

Figure 3-7. PPPoE Connection Setup

To complete the connection you must now click the Apply button. The Apply button will temporarily save this connection. To make the change permanent, click on

Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

PPPoA Connection Setup

PPPoA is defined in the Internet standard RFC 2364. It is a method of encapsulating PPP packets over ATM cells which are carried over the DSL line. PPP (Point-to-Point Protocol) is a method of establishing a network session between network hosts. It usually provides a mechanism of authenticating users. LLC and VC are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.

By selecting PPPoA, you are forcing your router to act as the termination point for the PPPoA connection. This frees up your PC resources and allows multiple users to utilize the PPPoA connection.

To configure the router for PPPoA:

► Procedure

1. Click on Setup and then click on New Connection. The default PPPoE connection setup is displayed.
2. At the Type field, select PPPoA from the drop-down list. The PPPoA connection setup page is displayed.
3. Give your PPPoA connection a unique name. The name must not have spaces and cannot begin with numbers.
4. Select or enter a VPI and VCI (as supplied by your DSL service provider or your ISP), or click in Auto PVC. (Auto PVC causes the router to perform automatic VPI/VCI detection as defined in DSL forum TR-068.)
5. Select NAT and Firewall if you want them active for this connection. Firewall and NAT services must be enabled. See Firewall/NAT Services on page 3-22.
6. Select the encapsulation type (LLC or VC); if you are not sure just use the default mode.
7. Select the quality of service (QoS). Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:
 - PCR (Peak Cell Rate)
 - SCR (Sustainable Cell Rate)
 - MBS (Maximum Burst Size)
 - CDVT (Cell Delay Variation Tolerance)

Following is a description of the different options:

- Username – The username for the PPPoA access. This is provided by your DSL service provider or your ISP.

- Password – The password for the PPPoA access. This is provided by your DSL service provider or your ISP.
- Idle Timeout – Specifies that PPPoA connection should disconnect if the link has no activity detected for the specified number of seconds. This field is used in conjunction with the On Demand feature. To disable the timeout feature, enter a zero in this field.
- Authentication – Specifies the authentication protocol: Auto (the protocol is selected by the PPPoA server), PAP (Password Authentication Protocol), or CHAP (Challenge Handshake Authentication Protocol).
- Keep Alive – When the On Demand option is not enabled, this value specifies the length of time to keep the connection from being shut down for inactivity by sending PPP LCP echoes to the PPP server. To ensure that the link is always active, enter a zero in this field.
- MTU – The Maximum Transmission Unit the DSL connection can send. It is a negotiated value. The maximum specified value is 1500, although some DSL/ISP providers require a larger value. The minimum MTU value is 128.
- On Demand – Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value.
- Default Gateway – Specifies whether a default gateway is used.
- Debug – Enables PPPoA connection debugging facilities.
- PPP Unnumbered – Specifies that the calling and answering routers will not request IP addresses.

The screenshot shows the Paradyne web interface for PPPoA Connection Setup. The navigation menu on the left includes: LAN Setup, LAN Configuration, Ethernet Switch, Firewall/NAT Services, WAN Setup, New Connection, Modem, TSM, Sample_Connection, and Log Out. The main configuration area is titled "PPPoA Connection Setup" and contains the following fields and options:

- Name: [Text Input]
- Type: PPPoA (Dropdown)
- Sharing: Disable (Button)
- Options: NAT Firewall
- VLAN ID: [Text Input]
- Priority Bits: [Text Input]
- PPP Settings**
 - Encapsulation: LLC VC
 - Username: useame
 - Password: ****
 - Idle Timeout: [Text Input] secs
 - Keep Alive: 1 min
 - Authentication: Auto CHAP PAP
 - MTU: 1500 bytes
 - On Demand: Default Gateway:
 - Debug:
 - PPP Unnumbered:
- PVC Settings**
 - PVC: New (Button)
 - VPI: [Text Input]
 - VCI: [Text Input]
 - QoS: UBR (Dropdown)
 - PCR: [Text Input] cps
 - SCR: [Text Input] cps
 - MBS: [Text Input] cells
 - CDVT: [Text Input] usecs
 - Auto PVC:

Buttons at the bottom include: Connect, Disconnect, Apply, Delete, and Cancel.

Figure 3-8. PPPoA Connection Setup

To complete the connection you must now click the Apply button. The Apply button will temporarily save this connection. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Static Connection Setup

A static connection is used whenever a known static IP is assigned. The accompanying information such as the subnet mask and the default gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers give you access to other web servers. The valid range of IP addresses is 1.0.0.0 to 223.255.255.254.

To configure the router for a Static connection:

► Procedure

1. Click on Setup and then click on New Connection. The default Static connection setup is displayed.
2. At the Type field, select Static. The Static Connection Setup page is displayed.
3. Give your Static connection a unique name. The name must not have spaces and cannot begin with numbers.
4. Optionally enable Network Address Translation (NAT) and the Firewall options. Firewall and NAT services must be enabled. See [Firewall/NAT Services](#) on page 3-22.
5. Select a PVC Sharing type of Disable, Enable, or VLAN.
6. Select or enter a VPI and VCI (as supplied by your DSL service provider or your ISP), or click in Auto PVC. (Auto PVC causes the router to perform automatic VPI/VCI detection as defined in DSL forum TR-068.) For VLAN, specify a VLAN ID and priority.
7. Select NAT and Firewall if you want them active for this connection. Firewall and NAT services must be enabled. See [Firewall/NAT Services](#) on page 3-22.
8. Select the encapsulation type (LLC or VC). If you are not sure which to use, just use the default mode.
9. Based upon the information your ISP provided, enter your assigned IP Address, Subnet Mask, Default Gateway (if provided), and Domain Name Services (DNS) address (if provided). Specify the VPI and VCI settings. Your DSL service provider or your ISP will supply these.
10. Select the quality of service (QOS). Leave the default value if your ISP did not provide this information.
11. Set the mode to Bridged or Routed as instructed by your ISP.

Figure 3-9. Static IP Connection Setup

To complete the connection you must now click the Apply button. The Apply button will temporarily save this connection. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

DHCP Connection Setup

Dynamic Host Configuration Protocol (DHCP) allows the router to automatically obtain the IP address from the server. This option is commonly used in situations where IP is dynamically assigned and is not known prior to assignment.

To configure the router for a DHCP connection:

► Procedure

1. Click on Setup and then click on New Connection. The default PPPoE connection setup is displayed.
2. At the Type field, select DHCP. The DHCP connection setup page is displayed.
3. Give your DHCP connection a unique name. The name must not have spaces and cannot begin with numbers.
4. Select a PVC Sharing type of Disable, Enable, or VLAN.
5. Select or enter a VPI and VCI (as supplied by your DSL service provider or your ISP), or click in Auto PVC. (Auto PVC causes the router to perform automatic VPI/VCI detection as defined in DSL forum TR-068.) For VLAN, specify a VLAN ID and priority.
6. Select NAT and Firewall if you want them active for this connection. Firewall and NAT services must be enabled. See [Firewall/NAT Services](#) on page 3-22.

7. Select the encapsulation type (LLC or VC). If you are not sure which to use, just use the default mode.
8. Select the quality of service (QoS). Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:
 - PCR (Peak Cell Rate)
 - SCR (Sustainable Cell Rate)
 - MBS (Maximum Burst Size)
 - CDVT (Cell Delay Variation Tolerance)

If your DSL line is connected and your DSL provider is supporting DHCP, you can click on the Renew button and the CPE will retrieve an IP Address, Subnet Mask, and Default Gateway address. At any time you can renew the DHCP address by clicking on the Renew button.

The screenshot shows the Paradyne web interface for DHCP Connection Setup. The navigation menu on the left includes LAN Setup, LAN Configuration, Ethernet Switch, Firewall/NAT Services, WAN Setup, New Connection, Modem, TSML, Sample Connection, and Log Out. The main content area is titled 'DHCP Connection Setup' and contains the following fields and options:

- Name: [text input]
- Type: DHCP [dropdown]
- Sharing: Disable [dropdown]
- Options: NAT Firewall
- VLAN ID: [text input]
- Priority Bits: [text input]
- DHCP Settings:
 - Encapsulation: LLC VC
 - IP Address: [text input]
 - Mask: [text input]
 - Gateway: [text input]
 - Default Gateway:
- PVC Settings:
 - PVC: [text input]
 - VPI: 0 [text input]
 - VCI: 0 [text input]
 - QoS: UBR [dropdown]
 - PCR: [text input] cps
 - SCR: [text input] cps
 - MBS: [text input] cells
 - CDVT: [text input] usecs
 - Auto PVC:

Buttons for Renew, Release, Apply, Delete, and Cancel are located at the bottom of the form.

Figure 3-10. DHCP Connection Setup

To complete the connection you must now click the Apply button. The Apply button will temporarily save this connection. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Bridged Connection

A pure bridged connection does not assign an IP address to the WAN interface. This connection method makes the router act as a hub that passes packets across the WAN interface to the LAN interface.

To configure the router as a bridge:

► Procedure

1. From the Home page, click on Setup and then click on New Connection. The default PPPoE connection setup is displayed.
2. At the Type field select Bridge. The Bridge connection setup page is displayed (see [Figure 3-11](#)).
3. Give your Bridge connection a unique name; the name must not have spaces and cannot begin with numbers.
4. Select a PVC Sharing type of Disable, Enable, or VLAN.
5. Select or enter a VPI and VCI. (Your DSL service provider or your ISP will supply these.) For VLAN, specify a VLAN ID and priority.
6. Select the encapsulation type (LLC or VC); if you are not sure which to use, just use the default mode.
7. Select the quality of service (QoS). Leave the default value if you are unsure or the ISP did not provide this information. Depending on the QoS you select, you may also enter:
 - PCR (Peak Cell Rate)
 - SCR (Sustainable Cell Rate)
 - MBS (Maximum Burst Size)
 - CDVT (Cell Delay Variation Tolerance)

The screenshot shows the 'Bridged Connection Setup' page in the Paradyne web interface. The left sidebar contains a navigation menu with categories like LAN Setup, WAN Setup, and New Connection. The main content area is titled 'Bridged Connection Setup' and includes the following fields and sections:

- Name:** A text input field.
- Type:** A dropdown menu set to 'Bridge'.
- Sharing:** A dropdown menu set to 'Disable'.
- VLAN ID:** A text input field.
- Priority Bits:** A text input field.
- Bridge Settings:**
 - Encapsulation: LLC VC
- PVC Settings:**
 - PVC: 1
 - VPI: 0
 - VCI: 0
 - QoS: UBR
 - PCR: 0 cps
 - SCR: 0 cps
 - MBS: 0 cells
 - CDVT: 0 usecs
 - Auto PVC:

At the bottom right, there are three buttons: 'Apply', 'Delete', and 'Cancel'.

Figure 3-11. Bridged Connection Setup

To complete the connection you must now click the Apply button. The Apply button will temporarily save this connection. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

CLIP Connection

Classical IP and ARP over ATM (CLIP) allows IP datagrams and ARP (Address Resolution Protocol) requests and replies to be transmitted over ATM using ATM Adaptation Layer 5 (AAL5).

To configure a CLIP connection:

► Procedure

1. From the Home page, click on Setup and then click on New Connection. The default PPPoE connection setup is displayed.
2. At the Type field select CLIP and the CLIP connection setup page is displayed.
3. Give your CLIP connection a unique name; the name must not have spaces and cannot begin with numbers.
4. Select or enter a VPI and VCI (as supplied by your DSL service provider or your ISP), or click in Auto PVC. (Auto PVC causes the router to perform automatic VPI/VCI detection as defined in DSL forum TR-068.)
5. Specify the IP address and subnet mask.
6. Specify the address of the ARP server.
7. Specify the address of the Default Gateway.
8. Select the quality of service (QoS). Leave the default value if you are unsure or the ISP did not provide this information. Depending on the QoS you select, you may also enter:
 - PCR (Peak Cell Rate)
 - SCR (Sustainable Cell Rate)
 - MBS (Maximum Burst Size)
 - CDVT (Cell Delay Variation Tolerance)

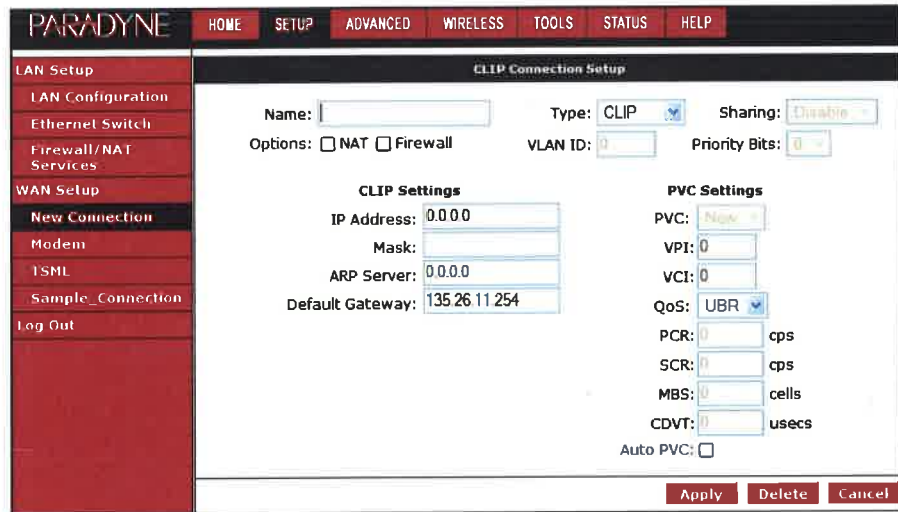


Figure 3-12. CLIP Connection Setup

To complete the connection you must now click the Apply button. The Apply button will temporarily save this connection. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Modify an Existing Connection

To modify an existing connection:

► Procedure

1. From the Home screen, click on Setup.
2. Click on the connection you want to modify. The connections are listed by name.

If you delete a connection, to make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Modem Setup

To configure the DSL modulation type:

► Procedure

1. From the Home screen, click on Setup.
2. Under WAN Setup, select Modem. This will bring up the Modem Setup screen. Leave the default value if your ISP did not provide this information. For most cases, this screen should not be modified.

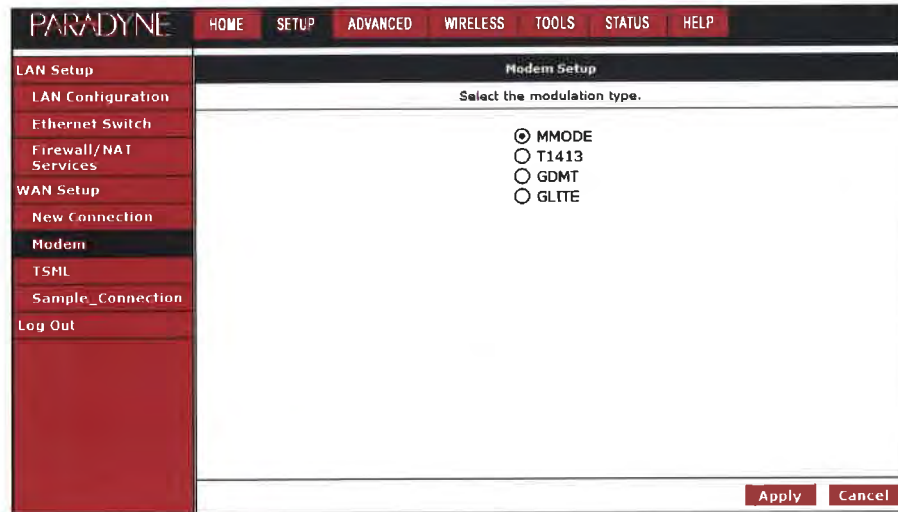


Figure 3-13. Modem Setup

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

TSML

Troubleshooting Management Link (TSML) is a feature that lets authorized Network Operations Center (NOC) personnel troubleshoot and manage the router from the NOC.

The TSML connection (VPI 0, VCI 34) examines incoming packets, looking for ICMP Echo Requests. If the TSML connection receives five ICMP Echo Request packets with the same destination IP address within five seconds, it adopts the destination IP address. The address can then be used to access the router.

The TSML connection is automatically configured. The TSML Connection screen shows the settings, but they cannot be altered and saved.

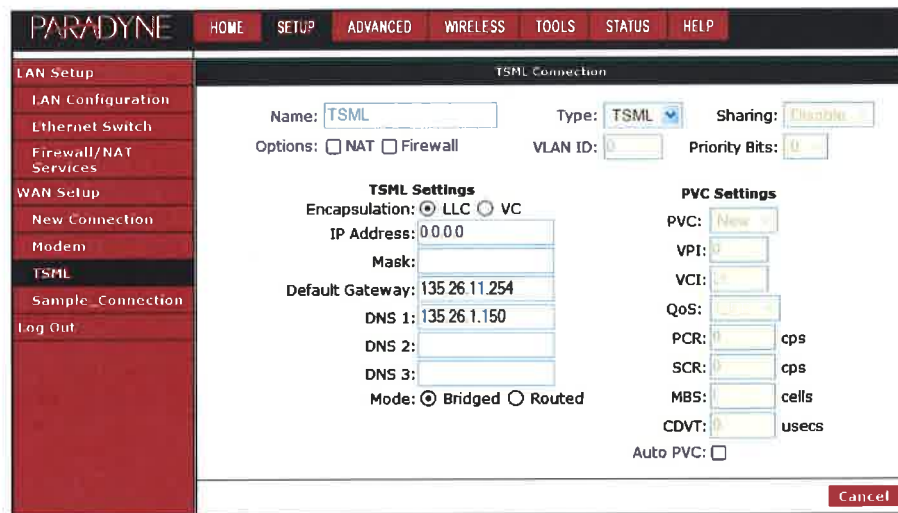


Figure 3-14. TSML Connection

Configuring the LAN

To configure LAN parameters, click on Setup on the Home screen. Under LAN Setup, click on LAN Configuration. The LAN Configuration screen appears.

Enable/Disable DHCP

By default, your CPE has DHCP server (LAN side) disabled. If you already have a DHCP server running on your network, do not enable a second DHCP server.

To enable DHCP:

► Procedure

1. From the Home screen, click on Setup.
2. Under LAN Setup, select LAN Configuration. The LAN Group 1 Configuration screen appears.

The screenshot shows the PARADYNE web interface. The top navigation bar includes HOME, SETUP, ADVANCED, WIRELESS, TOOLS, STATUS, and HELP. The left sidebar menu lists LAN Setup, LAN Configuration, Ethernet Switch, Firewall/NAT Services, WAN Setup, New Connection, Modem, TSM, Sample_Connection, and Log Out. The main content area is titled 'LAN Group 1 Configuration'. It features three radio button options under 'IP Settings': 'Obtain an IP address automatically', 'PPP IP Address', and 'Use the following Static IP address'. The 'Use the following Static IP address' option is selected. Below this, there are input fields for IP Address (192.168.1.1), Netmask (255.255.255.0), Default Gateway (135.26.11.254), Host Name (mygateway1), and Domain (ar7). There are also 'Release' and 'Renew' buttons. Underneath, the 'Enable DHCP Server' option is selected with a radio button. This section includes input fields for Start IP (192.168.1.2), End IP (192.168.1.254), and Lease Time (3600 Seconds). Other options include 'Enable DHCP Relay' with a 'Relay IP' field (192.168.1.1) and 'Server and Relay Off'. To the right, a 'Services' section lists IP Filters, Bridge Filters, UPnP, LAN Clients, IP QoS, and Static Routing, each with a status indicator. A 'Status' section shows colored indicators for each service. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Figure 3-15. LAN Group 1 Configuration

3. The DHCP server is enabled when "Enable DHCP Server" is selected. If you enable it:
 - Specify a Start IP address. The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the router's IP address value. For example, if the router's IP address is

192.168.1.1 (the default) than the Start IP address must be 192.168.1. 2 or higher.

- Specify an End IP address. The End IP Address is the last address the DHCP server can issue. The ending address cannot exceed a subnet limit of 254. The maximum IP address for a router using the default address is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users will not get access to network resources.
- Specify a Lease Time. The Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. The amount of time is in units of seconds; the default value is 3600 seconds (1 hour).

Note: If you change the start or end values, make sure the values are still within the same subnet as the router's IP address. For example, if the router's IP address is 192.168.1.1 (the default), and you change the DHCP Start and End IP addresses to be 192.128.1.2 and 192.128.1.100, you will not be able to communicate with the router if your PC has DHCP enabled.

In addition to the DHCP server feature, the router supports the DHCP relay function. When the router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the router is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.

If the DHCP server and relay are turned off, you must configure the IP address, subnet mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer. Your router must be on the same subnet as the computers.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Changing the Router's IP address

Your router's default IP address and subnet mask are 192.168.1.1 and 255.255.255.0, respectively. This subnet mask allows the router to support 254 users. Since the DHCP server issues a maximum of 255 addresses, there is not much advantage to changing the subnet mask to increase the number of addresses. Further, remember that if you change your router's IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet.

The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway address.

The Hostname can be any alphanumeric word beginning with a letter and containing no spaces. The domain name is used to in conjunction with the host name to uniquely identify the router.

To change the router's IP address:

► Procedure

1. From the Home screen, click on Setup.
2. Under LAN Setup, select LAN Configuration. The LAN Group 1 Configuration screen appears, as shown in [Figure 3-15, LAN Group 1 Configuration](#).
3. Click on “Use the following Static IP Address”.
4. Enter a new IP Address and Netmask.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Ethernet Switch

To set the speed and duplex mode of the LAN ports:

► Procedure

1. From the Home screen, click on Ethernet Switch. The Ethernet Switch screen appears.
2. For Physical Port1 through Physical Port4 (LAN1 through LAN4), select a mode and speed from the Set Value drop-down list. Select Auto to negotiate the Ethernet duplex mode and speed with attached equipment that supports auto-negotiation.

The current configured or negotiated settings are displayed under Fallback Value.

The Apply button will temporarily save the Ethernet Switch settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

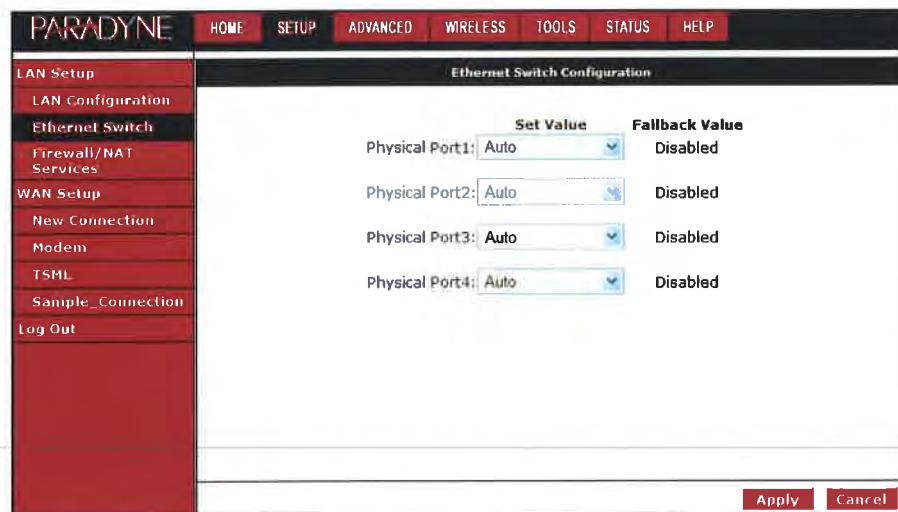


Figure 3-16. Ethernet Switch

Firewall/NAT Services

To enable or disable Firewall and NAT:

► Procedure

1. From the Home screen, click Setup.
2. Under LAN Setup, select Firewall/NAT Services. By unselecting the Enable Firewall and NAT Services button the firewall and NAT services is disabled for all WAN connections. Enabling Firewall NAT does not automatically apply it to connections.

The Apply button will temporarily save this setting. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

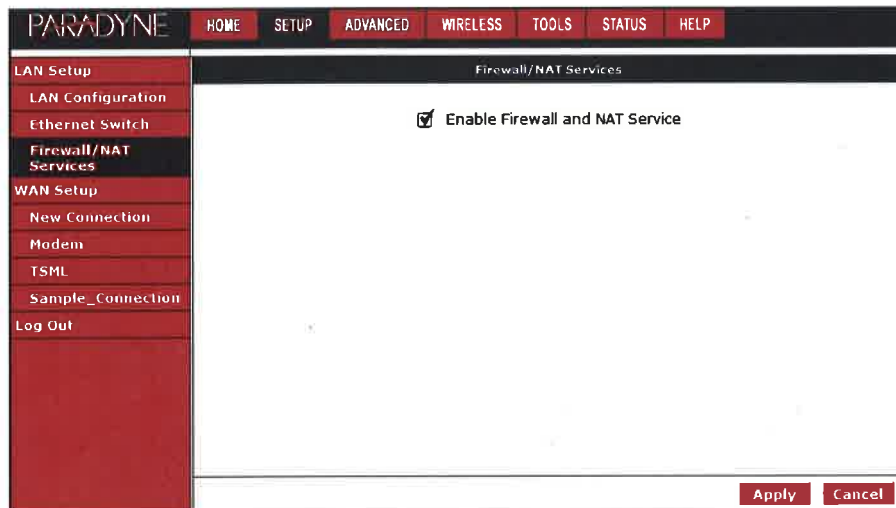


Figure 3-17. Firewall/NAT Services

Advanced

The CPE supports a host of advanced features. For basic router functionality, you do not need to utilize these advanced features. The features help with routing, security, port configuration, and plug and play capability.

UPnP

UPnP NAT and Firewall Traversal allow traffic to pass through the router for applications using the UPnP protocol. This feature requires one active DSL connection. In the presence of multiple DSL connections, select the one over which the incoming traffic will be present, such as the default Internet connection.

To enable UPnP you must first have a WAN connection configured. Once a WAN connection is configured:

► Procedure

1. From the Home screen, click on Advanced and under Advanced, select UPnP. The UPnP screen appears.
2. Enable UPnP and then select which connection will utilize UPnP.
3. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

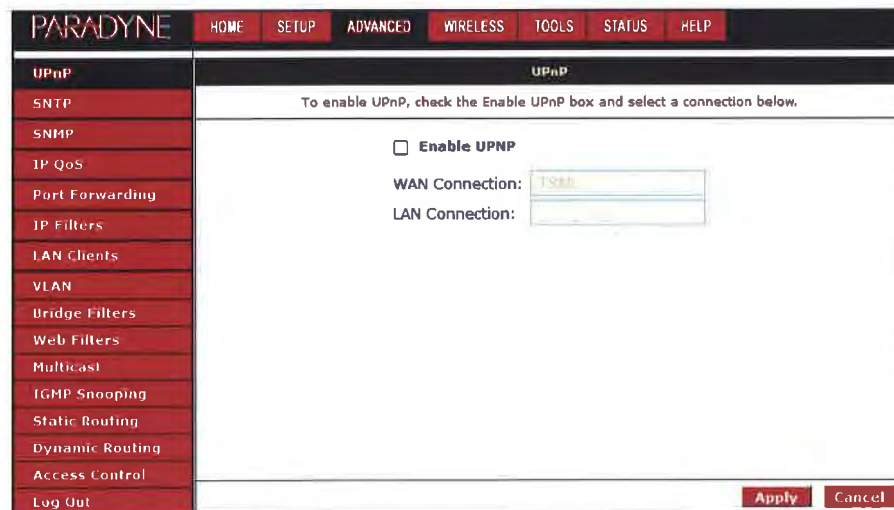


Figure 3-18. UPnP

SNTP

The SNTP screen lets you specify parameters related to SNTP (Simple Network Time Protocol) servers. To use SNTP:

► Procedure

1. From the Home screen, click on Advanced and under Advanced, select SNTP. The SNTP screen appears.
2. Enable SNTP and then specify one or more SNTP servers.
3. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

Figure 3-19. SNTP

SNMP

Use the SNMP (Simple Network Management Protocol) screen to enable and configure the SNMP agent and SNMP trap managers.

The SNMP feature generates a trap whenever the IP address of the router changes (except through the Troubleshooting Management Link). The trap sent contains the following:

- Community ("public")
- sysObjectID for the router
- IP address of the agent sending the trap
- Time stamp (sysUpTime)
- Serial Number of the router
- IP address of the router
- Interface name

To configure SNMP:

► Procedure

1. From the Home screen, click on Advanced and under Advanced, select SNMP. The SNMP screen appears.
2. Enable the SNMP traps, then enter up to five Destination IP Addresses and Community names.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

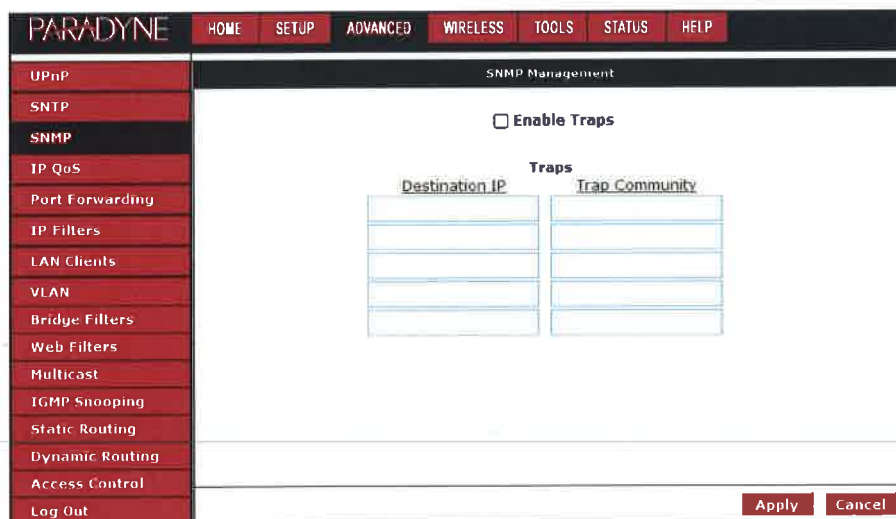


Figure 3-20. SNMP

IP QoS

The IP QoS screen lets you establish a particular level of service for each connection you have defined. To set QoS for a connection:

► Procedure

1. From the Home screen, click on Advanced and under Advanced, select IP QoS. The IP QoS screen appears.
2. Select a connection from the drop-down list and enter or select appropriate options.
3. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

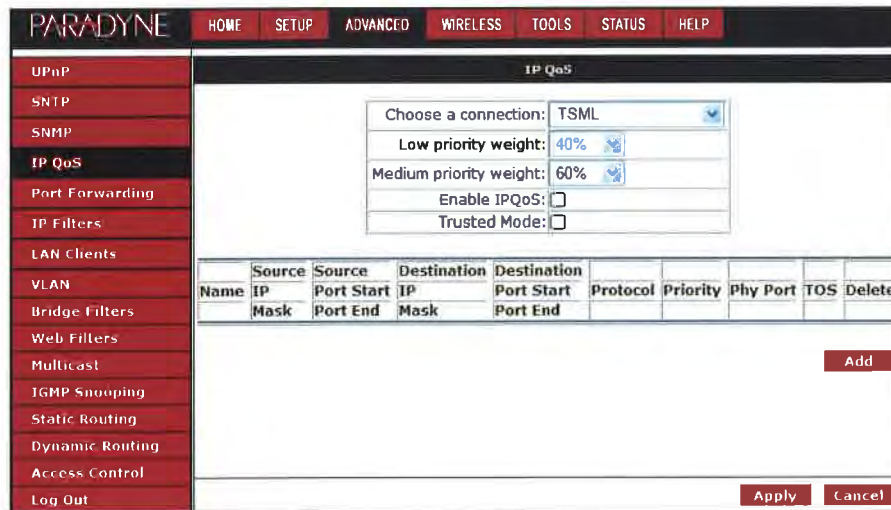


Figure 3-21. IP QoS

Port Forwarding

Using the Port Forwarding page you can provide local services (such as web hosting) for people on the Internet. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC. Port forwarding can be used with DHCP-assigned addresses, but remember that a DHCP address is dynamic. If you were configuring a Netmeeting server, for example, you would want to assign this server a static IP address so that the IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. The port forwarding feature will translate the WAN IP address into a LAN IP address.

You can use the LAN Clients screen to reserve an IP address for a DHCP client. See [LAN Clients](#) on page 3-29.

To configure a service, game, or other application:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Port Forwarding.
3. Select the computer hosting the service and add the corresponding firewall rule.
4. If you want to add a custom application, select the User category, click on New, and fill in the port, protocols and description for your application.

For example, if you want to host a Netmeeting session, from the Home screen, click on Advanced and under Advanced, select Port Forwarding. First select the IP address for your Netmeeting server. Next select the Audio/Video category and add Netmeeting to the Applied Rules box. To view the management rules, highlight Netmeeting and select view. This will display the preconfigured protocols and ports that Netmeeting will use. Now you can run Netmeeting from your server and call users that are on the Internet. If they know your WAN IP address, users can call you.

5. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

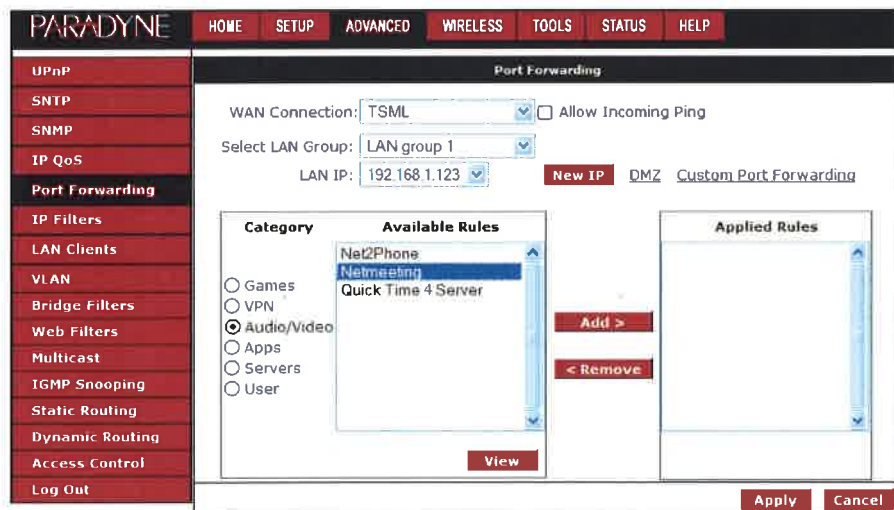


Figure 3-22. Port Forwarding: Netmeeting

IP Filters

Use the IP Filters screen to block all or selected traffic. To set up IP Filters:

► Procedure

1. From the Home screen, click on Advanced and under Advanced, select IP Filters. The IP Filters screen appears.
2. Select the LAN Group from the drop-down list that these changes will apply to.
3. Select a LAN IP address from the LAN IP drop-down list. Click on New IP to add a new IP address to the list.
4. Select available rules from the list, or click on Custom IP Filters to create a new rule.
5. Click on Apply. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

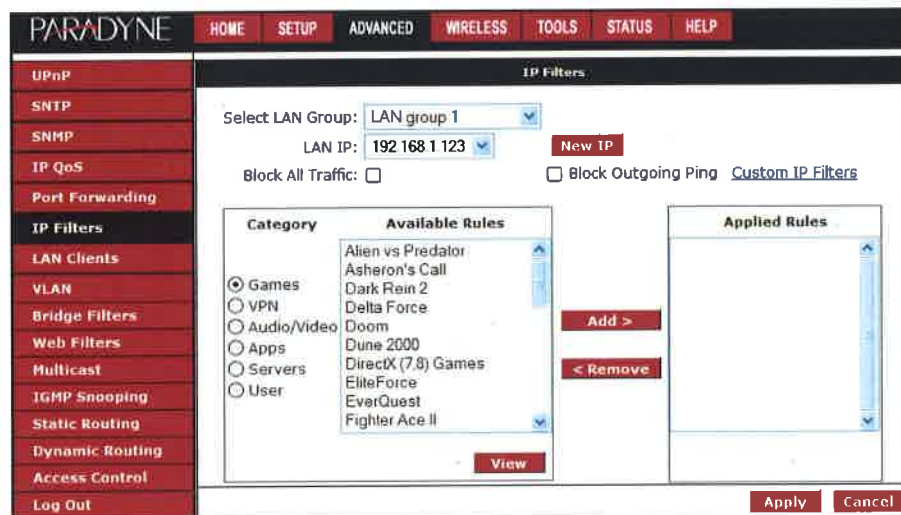


Figure 3-23. IP Filters

LAN Clients

To add a LAN client, or reserve an IP address for a DHCP client:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select LAN Clients. If DHCP is used, all DHCP clients are automatically assigned. If a fixed IP address server is on the LAN and you want this server to be visible via the WAN, you must add its IP address. Once the IP address has been added to you can apply Port Forwarding rules to this IP address.
3. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

Delete	IP Address	Hostname	MAC	Type
<input type="checkbox"/>	192.168.1.123	myhost.com		Static

Figure 3-24. LAN Clients

VLAN

You can use the VLAN (Virtual Local Area Network) screen to match different VLAN IDs to the LAN ports.

To configure VLANs:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select VLAN. The VLAN screen appears.
3. Click the appropriate buttons to assign VLAN IDs to the LAN ports.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

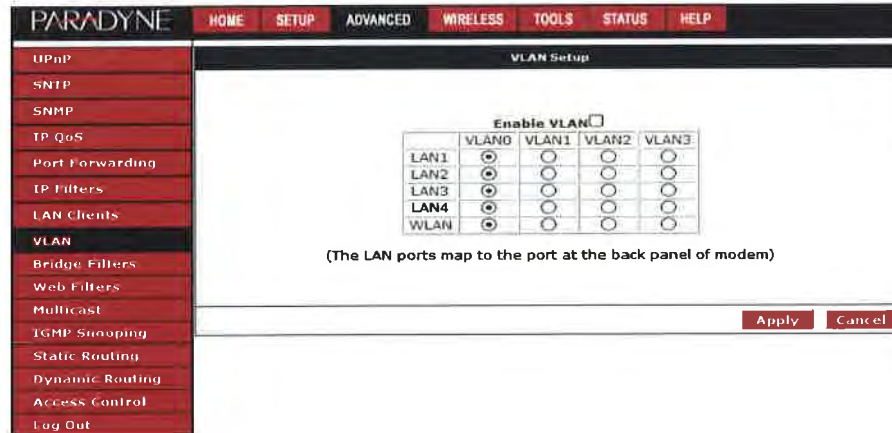


Figure 3-25. VLAN

Bridge Filters

The bridge filtering mechanism provides a way for the users to define rules to allow or deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the defined filter rules sequentially, and when a matched is determined, the appropriate filtering action (allow or deny) is performed. The bridge filter will only examine frames from interfaces which are part of the bridge itself. Twenty filter rules are supported with bridge filtering.

To enable Bridge Filters:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Bridge Filters. The Bridge Filters screen appears, as shown in [Figure 3-26, Bridge Filters](#).

The User Interface for Bridge Filter allows the user to add, edit, and delete, as well as enable the filter rules. To add rules, define the source MAC address, destination MAC address, and frame type with the desired filtering action (allow or deny), and click on the Add button. The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 or blanks meaning any address.

To edit or modify an existing filter rule, select the desired rule created previously in the Edit select box. The selected filter rule appears in the top section, as with the Add procedure. Make the desired change to the MAC address, frame type and access type, and click on Apply.

To delete a filter rules, select the filter rule entry to delete in the Delete selection box. Note that multiple deletions are possible. Once all the desired filter rules are selected for deletion, click on the Apply button. The Select All select box can also

be used to delete the entire filter rule. It provides a quick method of selecting all filter rules for deletion.

The Enable Bridge Filters button allows you to enable or disable bridge filtering. It can be set or unset during any add, edit, or delete operation. It can also be set or unset independently by pressing the Apply button.

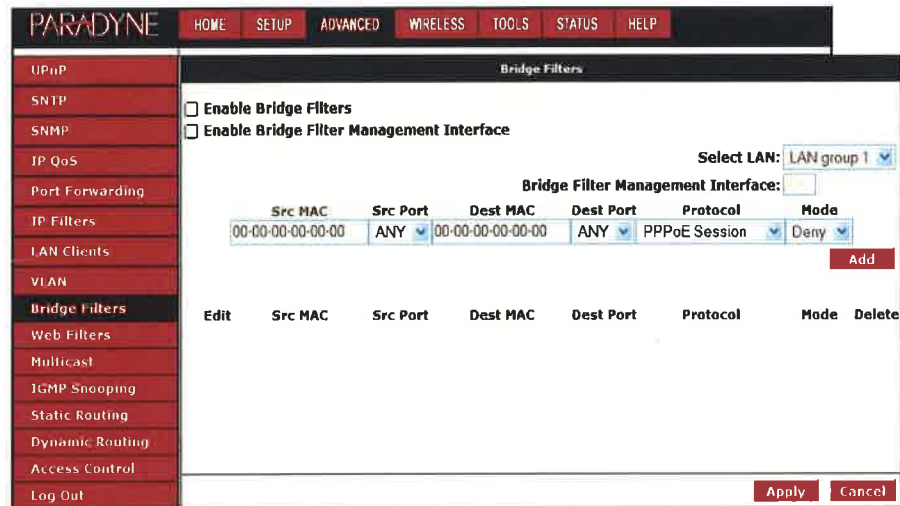


Figure 3-26. Bridge Filters

Note: The bridge filter table contains three hidden rules. These rules are entered automatically by the system to ensure that you don't lock yourself out of the system. The first rule allows all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the router to go through. The third rule allows all IPv4 frames with the source MAC address of the router to go through.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

Note: On a windows based machine, you can find a MAC address with the ipconfig program. At a command prompt, type: ipconfig /all

Web Filters

This option enables the IGMP proxy, which allows NAT clients to participate in IGMP multicast groups. It should only be enabled if NAT is also enabled.

To enable Multicasting:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Web Filters.
3. Select features to be enabled and disabled over the router.
4. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

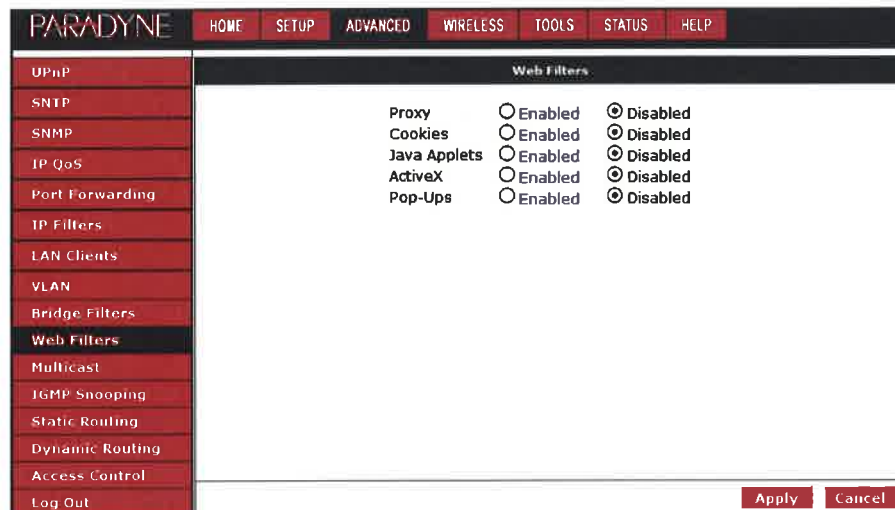


Figure 3-27. Web Filters

Multicast

This option enables the IGMP proxy, which allows NAT clients to participate in IGMP multicast groups. It should only be enabled if NAT is also enabled.

To enable Multicasting:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Multicast.
3. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

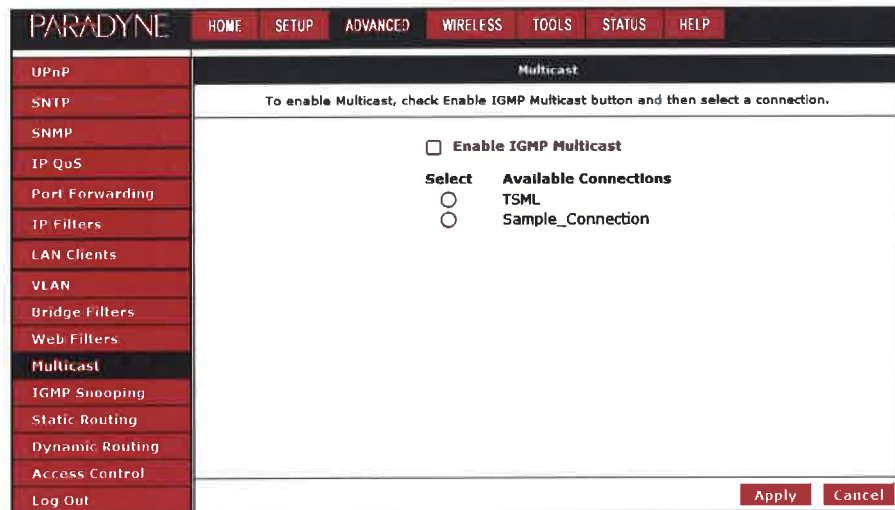


Figure 3-28. Multicast

IGMP Snooping

Use the IGMP Snooping screen to specify whether IGMP Snooping is enabled. When IGMP Snooping is enabled, the router analyzes Internet Group Management Protocol (IGMP) packets to learn multicast group address and port associations.

To enable IGMP Snooping:

1. From the Home screen, click on Advanced.
2. Under Advanced, select IGMP Snooping.
3. Click in the check box to enable snooping.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

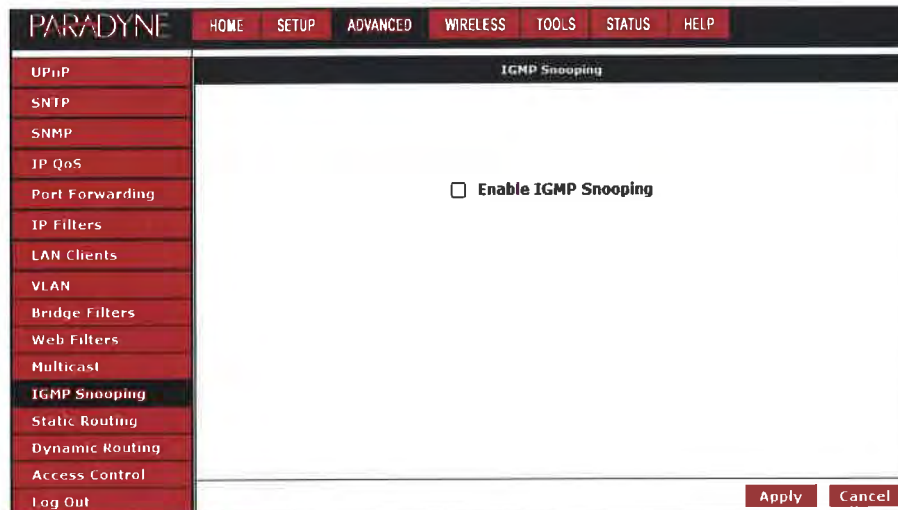


Figure 3-29. IGMP Snooping

Static Routing

If the router is connected to more than one network, you may need to set up a static route between the networks. A static route is a predefined pathway that network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the router.

To enable Static Routing:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Static Routing.

3. Specify the New Destination IP. This is the address of the remote LAN network or host to which you want to assign a static route. Enter the IP address of the host for which you wish to create a static route here. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0. The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0.
4. Specify the Gateway address. This is the IP address of the device that allows contact between the router and the remote network or host.
5. Specify the Metric. This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network (such as a router or switch).
6. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

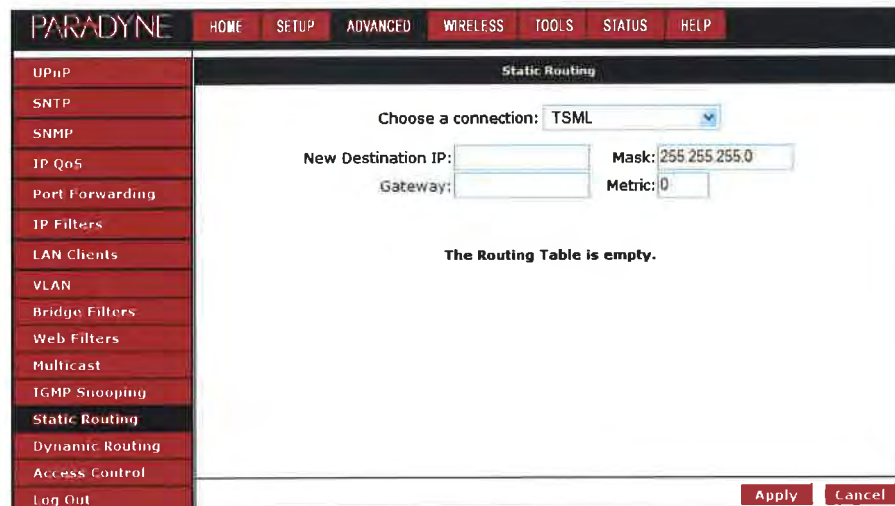


Figure 3-30. Static Routing

Dynamic Routing

Dynamic Routing allows the CPE to automatically adjust to physical changes in the network. The CPE, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network.

To enable Dynamic Routing:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Dynamic Routing.

3. Specify the Protocol. The protocol is dependent upon the entire network. Most networks support RIP v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If RIP v2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If Rip v1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting.
4. Specify the Direction. This determines the direction that RIP routes will be updated. Selecting In means that the router will only incorporate received RIP information. Selecting Out means that the router will only send out RIP information. Selecting both means that the router will incorporate received RIP information and send out updated RIP information.
5. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

The screenshot shows the Paradyne web interface for Dynamic Routing configuration. The top navigation bar includes HOME, SETUP, ADVANCED, WIRELESS, TOOLS, STATUS, and HELP. The left sidebar lists various configuration options, with 'Dynamic Routing' highlighted. The main content area is titled 'Dynamic Routing' and contains the following settings:

- Enable RIP
- Protocol: RIP v2 (dropdown menu)
- Enable Password
- Password: **** (text input)

Interface	Direction
LAN group 1	Both (dropdown menu)
Sample_Connection	Both (dropdown menu)

At the bottom right of the configuration area, there are 'Apply' and 'Cancel' buttons.

Figure 3-31. Dynamic Routing

Access Control

Access control allows certain PCs to access the router after the firewall is enabled.

Access control is enabled on a WAN connection only if the firewall is enabled globally (see [Firewall/NAT Services](#) on page 3-22) and enabled on that WAN connection.

To enable any of the Access Control features:

► Procedure

1. From the Home screen, click on Advanced.
2. Under Advanced, select Access Control. The Access Control screen appears. All Access Control rules have precedence over rules that were added via the Port Forwarding page.
3. The Apply button will temporarily save these settings. To make the change permanent, click on Tools and select System Commands. On the System Commands page, click on Save All.

Service Name	WAN	LAN group 1
Telnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Web	<input type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TFTP	<input type="checkbox"/>	<input type="checkbox"/>
Secure Shell (SSH)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SNMP	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3-32. Access Control

Log Out

Click on Log Out to close the session.

Wireless

The Wireless tab provides access to screens that let you configure parameters related to the router's wireless LAN connection.

Setup

The Wireless Setup screen contains the wireless LAN user settings.

To change the Wireless Setup:

► Procedure

1. From the Home screen, click on the Wireless tab.
2. From the Wireless menu, click on Setup. The Wireless Setup screen appears.
3. Enter or select the parameters described in [Table 3-2, Wireless Setup](#).

Figure 3-33. Wireless Setup Screen

Table 3-2. Wireless Setup (1 of 2)

Parameter	Description
Enable AP	Enabling the Access Point (AP) turns on the router's wireless capability. To use wireless devices, verify that the box is checked.
SSID	Specify the Service Set Identifier (SSID) for your wireless LAN. It can be up to 32 characters and cannot include spaces.
Hidden SSID	Enable Hidden SSID by clicking in the check box. When Hidden SSID is enabled, the SSID is not advertised. Users must know the SSID to connect to the wireless LAN.

Table 3-2. Wireless Setup (2 of 2)

Parameter	Description
Channel B/G	Specify the RF (Radio Frequency) channel (1–11) for the router to use. Recommended values are 1, 6, and 11. These three values do not overlap and could be used by three neighboring wireless LANs.
802.11 Mode	Specify whether the router will support only 802.11b (11 Mbps) clients, only 802.11b+ clients (22 Mbps), only 802.11g (54 Mbps) clients, or all. To allow any client to connect, select Mixed.
4X	Enable 4X mode only if all clients that will connect to the wireless LAN support 802.11b+.
User Isolation	Select if you want to forbid communication between users on the wireless LAN.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All. Then turn off and turn on the router to put the settings into effect.

Configuration

The Wireless Configuration screen contains the wireless LAN operational settings. Do not change anything on the Wireless Configuration screen unless you are so directed by your ISP.

To view the Wireless Configuration settings:

► Procedure

1. From the Home screen, click on the Wireless tab.
2. From the Wireless menu, click on Configuration. The Wireless Configuration screen appears.

Figure 3-34. Wireless Configuration Screen

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All. Then turn off and turn on the router to put the settings into effect.

Security

The Wireless Security screen contains the settings for applying security to your wireless LAN.

To change Wireless Security:

► Procedure

1. From the Home screen, click on the Wireless tab.
2. From the Wireless menu, click on Security. The Wireless Security screen appears.

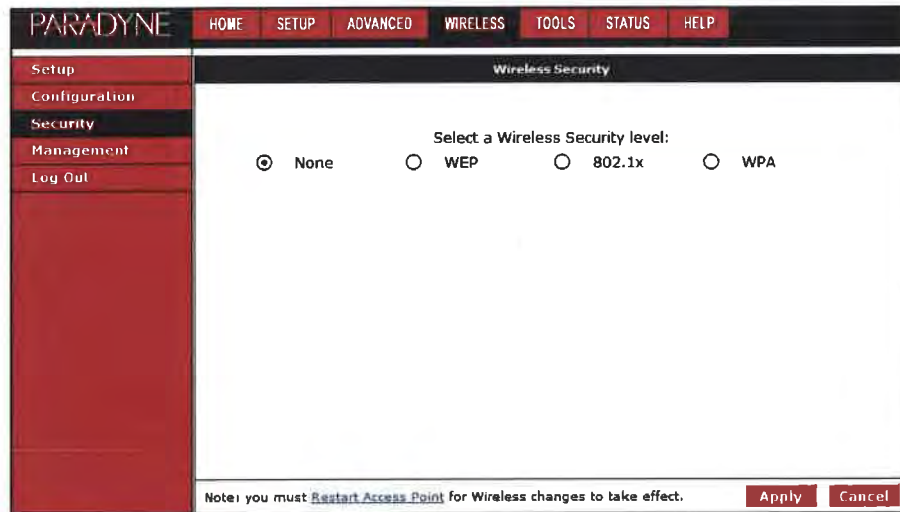


Figure 3-35. Wireless Security Screen

3. Select a security type:

- None. Anyone can connect to the wireless LAN.
- WEP (Wired Equivalent Privacy). Users of the wireless LAN must supply an encryption key, as defined on this screen. If an Authentication Type of Shared is selected, the client must properly encrypt a packet sent by the router using the encryption key; however, this method allows hackers to deduce the key. An Authentication Type of Open is recommended.



Figure 3-36. Wireless Security WEP Screen

- 802.1x. This security level uses a RADIUS (Remote Authentication Dial-In User Service) authentication server to manage network access. Specify

the address of the RADIUS server, the Port, the shared Secret, and the Interval in seconds at which authentication must be repeated.

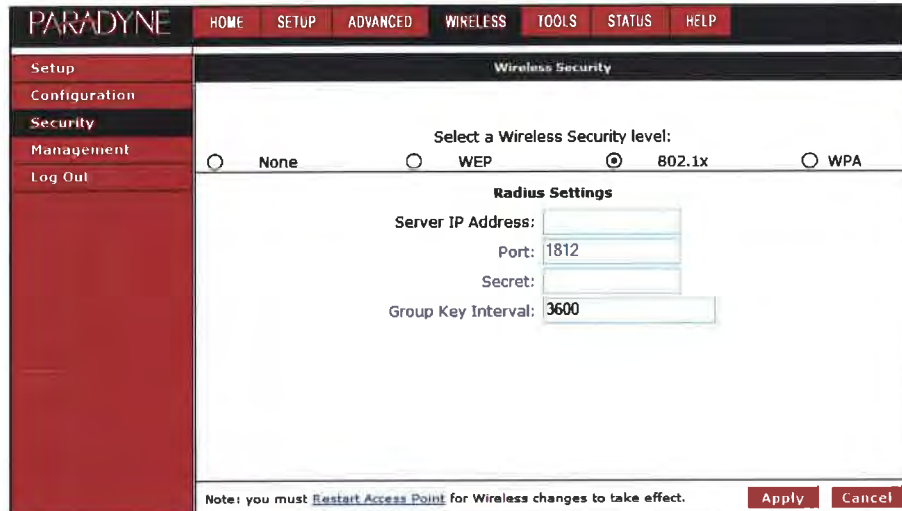


Figure 3-37. Wireless Security 802.11x Screen

- WPA (Wi-Fi Protected Access). For WPA you can specify a RADIUS server (as with 802.1x, above) or a Pre-Shared Key (PSK).

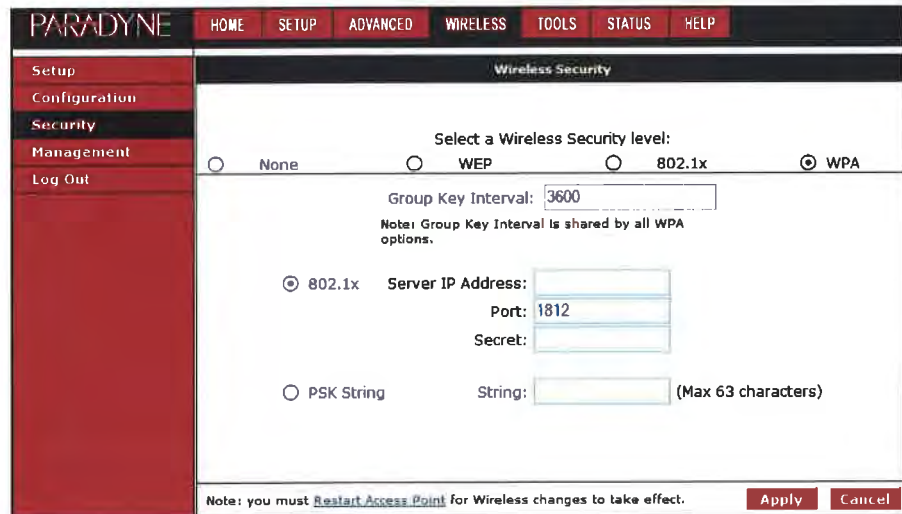


Figure 3-38. Wireless Security WPA Screen

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All. Then turn off and turn on the router to put the settings into effect.

Management

The Wireless Management screen allows you to control access, display clients, and establish multiple SSIDs.

To use Wireless Management:

► Procedure

1. From the Home screen, click on the Wireless tab.
2. From the Wireless menu, click on Management. The Wireless Management screen appears.
3. Select:
 - Access List – To allow or deny access to the wireless LAN by MAC address. Enable the access list, then add allowed or denied MAC addresses.

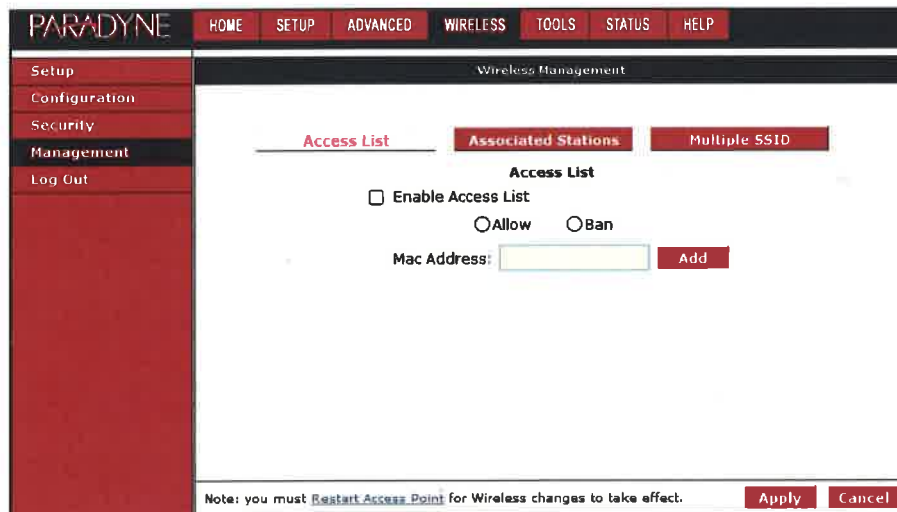


Figure 3-39. Wireless Management Access List Screen

- Associated Stations – To display wireless clients currently connected to the router.

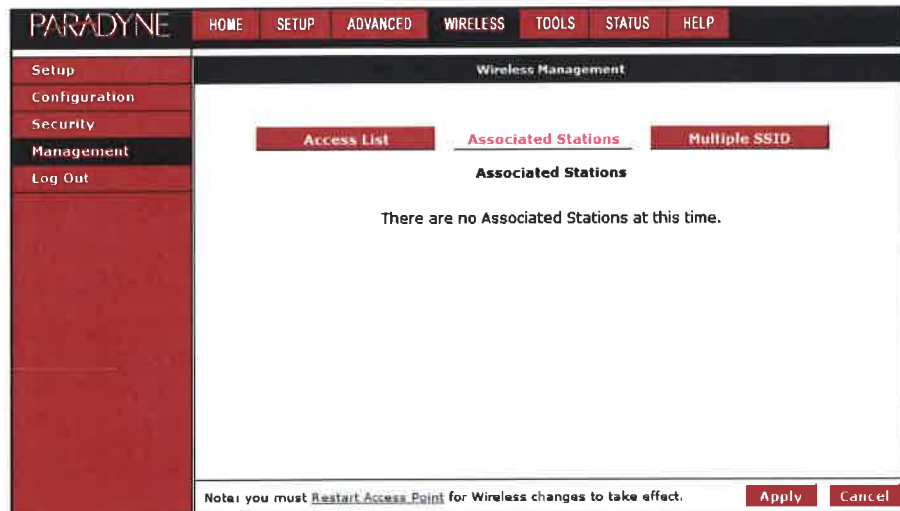


Figure 3-40. Wireless Management Associated Stations Screen

- Multiple SSIDs – To cause the router to advertise the wireless LAN using more than one Service Set Identifier (SSID).

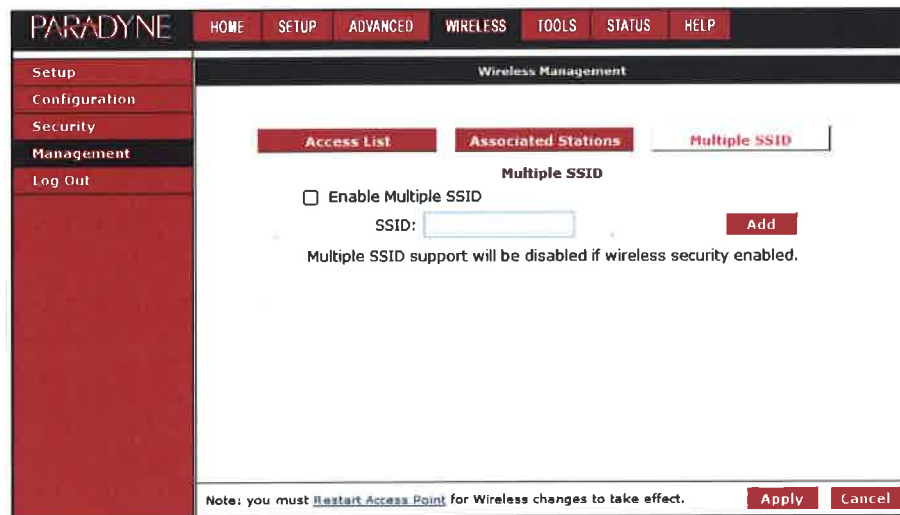


Figure 3-41. Wireless Management Multiple SSID Screen

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All. Then turn off and turn on the router to put the settings into effect.

Tools

The Tools tab provides access to system commands and functions.

System Commands

To make changes permanent, click on Tools (at the top of the page) and select System Commands. The following commands are used to configure the router:

- **Save All:** Click on this button in order to permanently save the current configuration of the router. If you do restart the system without saving your configuration, the CPE will revert back to the previously saved configuration.
- **Restart:** Use this button to restart the system. If you have not saved your configurations, the router will revert to the previously saved configuration upon restarting. Connectivity to the unit will be lost. You can reconnect after the unit reboots.
- **Restore Defaults:** Use this button to restore the default settings selected by your service provider. Connectivity to the unit will be lost. You can reconnect after the unit reboots.

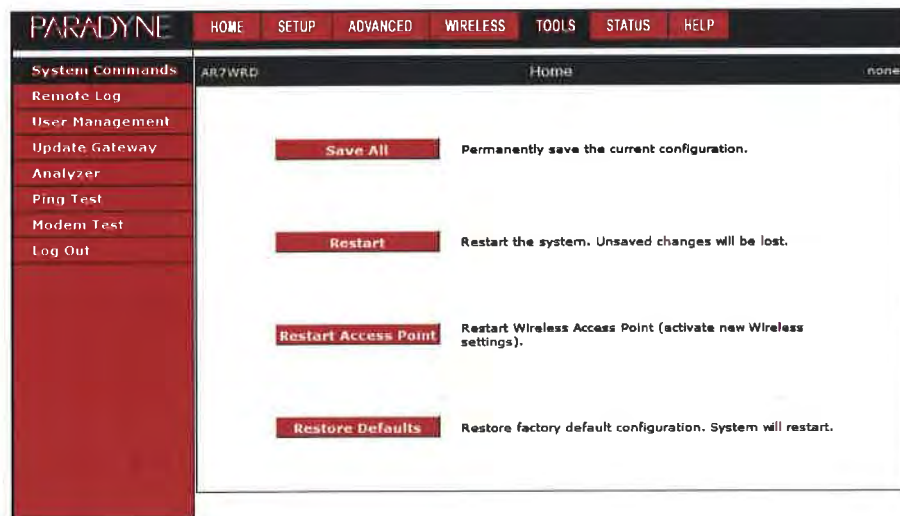


Figure 3-42. System Commands

Remote Log

The remote log feature forwards all logged information to a remote PC. The type of information forwarded to the remote PC depends upon the log level. Each log message is assigned a severity level, which indicates how seriously the triggering event affects router functions. When you configure logging, you must specify a severity level for each facility. Messages that belong to the facility and are rated at that level or higher are logged to the destination.

For PPPoE and PPPoA connections, you can select Debug if you want to log the connection information. This is helpful when trying to debug connection problems.

Table 3-3 defines the different severity levels.

Table 3-3. Severity Levels

Severity Level	Description
Panic	System panic or other condition that causes the router to stop functioning.
Alert	Conditions that require immediate correction, such as a corrupted system database.
Critical	Potentially critical conditions, such as hard drive errors.
Error	Error conditions that generally have less serious consequences than errors in the panic, alert, and critical levels.
Warning	Conditions that warrant monitoring.
Notice	Conditions that are not errors but might warrant special handling.
Info	Events or non-error conditions of interest.
Debug	Software debugging messages. Specify this level only if so directed by your technical support representative.

To forward logging information:

► Procedure

1. Click on Tools and select Remote Log.
2. Select a Log Level from the drop-down list.
3. Type the IP address of the remote logging destination and click on Add.
4. Click on Apply. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

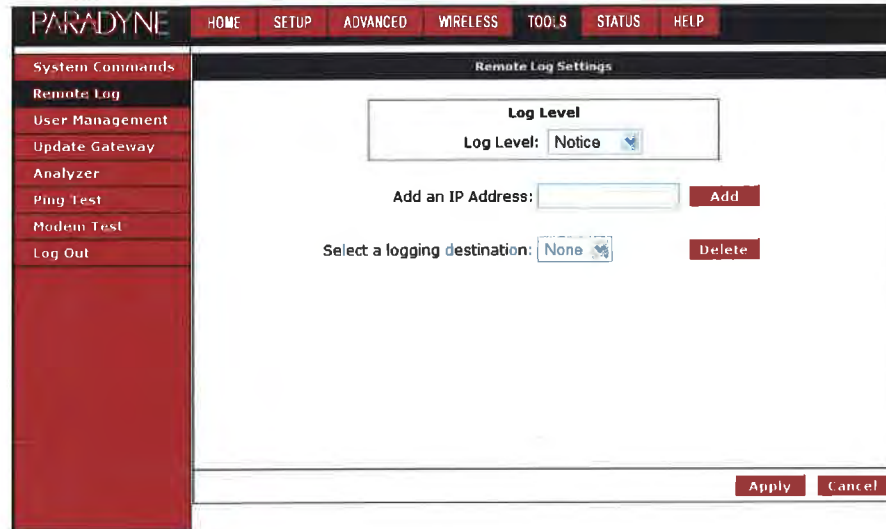


Figure 3-43. Remote Log

User Management

To change your router's username and password:

► Procedure

1. From the Home screen, under the tools menu, click on User Management.
2. Change the login name and password.
3. If desired, you can change the idle timeout from this screen. The idle timeout determines after how many minutes of inactivity the web interface is logged off.

The Apply button will temporarily save these settings. To make the change permanent, click on Tools (at the top of the page) and select System Commands. At the System Commands page, click on Save All.

If you forget your password, you can press and hold the reset to factory defaults button for 10 seconds. The router will be reset to its factory default configuration and all custom configurations will be lost.

The screenshot shows the Paradyne web interface. At the top, there is a navigation bar with tabs: HOME, SETUP, ADVANCED, WIRELESS, TOOLS, STATUS, and HELP. On the left side, there is a vertical menu with the following items: System Commands, Remote Log, User Management (highlighted), Update Gateway, Analyzer, Ping Test, Modem Test, and Log Out. The main content area is titled 'User Management' and contains the following text and form fields:

User Management is used to change your User Name or Password.

User Name:

Password:

Confirmed Password:

Idle Timeout: minutes

At the bottom right of the form, there are two buttons: Apply and Cancel.

Figure 3-44. User Management

Update Gateway

You can remotely upgrade the router's firmware from the web interface.

To upgrade the firmware:

► Procedure

1. From the Home screen, under the Tools title, click on Update Gateway.
2. Click on Browse, and find the firmware file to download. Make sure this is the correct file.
3. Click on upgrade firmware. Once the upgrade is complete the CPE will reboot. You will need to log back onto the CPE after the firmware upgrade is complete.

The firmware upgrade should take less than 5 minutes to complete. If it takes longer than 5 minutes, something has gone wrong.

Caution: Do not remove power from the router during the firmware upgrade procedure.

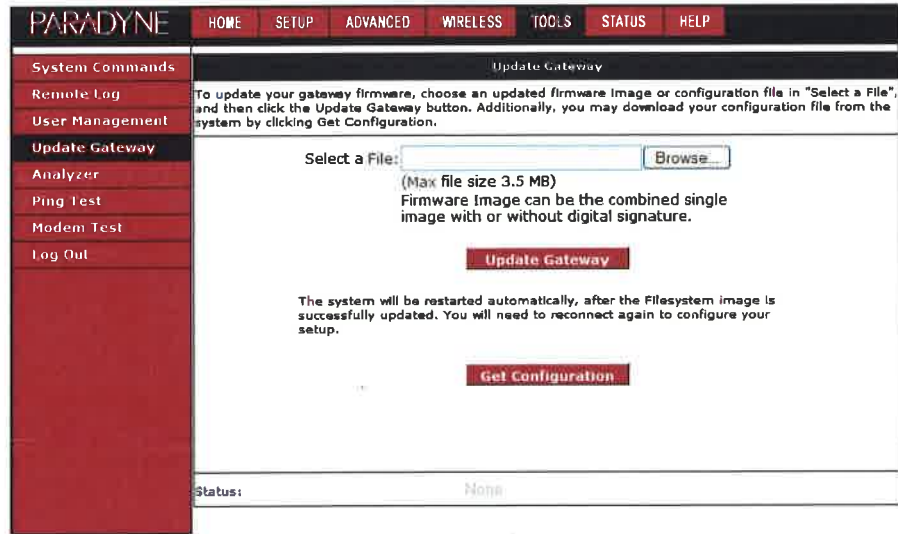


Figure 3-45. Update Gateway

Analyzer

The Analyzer screen shows link statuses and test results.

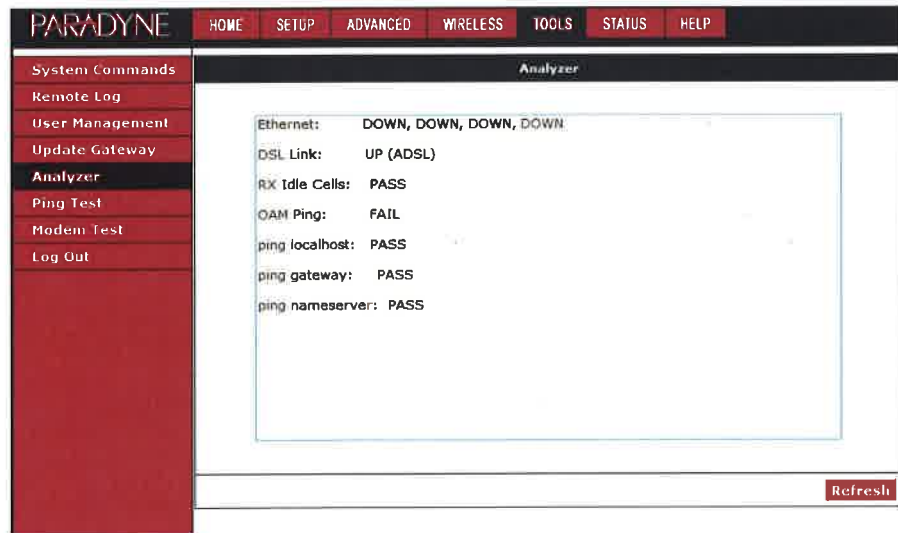


Figure 3-46. Analyzer

Ping Test

Once you have your router configured, it is a good idea to make sure you can ping the network. If you have your PC connected to the router via the default DHCP configuration, you should be able to ping the network address 192.168.1.2. If your ISP has provided their server address you can try to ping that address. If the pings for both the WAN and the LAN side are successful, and you have the proper protocols configured, you should be able to access the Internet.

To run a ping test:

► Procedure

1. From the Home screen, under the Tools title, click on Ping Test.
2. Specify the target IP Address that you want to ping.

Optionally, specify:

- TOS Byte value. This is part of the IP header of the ping packet. Valid values are 0 to 255.
- Packet size. Valid values are 36 to 65507.
- Number of echo requests. Valid values are 1 to 9.

3. Click on Test.

By default, when you select ping test, the router will ping itself three times. In [Figure 3-47](#), the router passed the Ping Test; this basically means that the TCP/IP protocol is up and running. If this first test does not pass, the TCP/IP protocol is not loaded. In this case, restart the router.

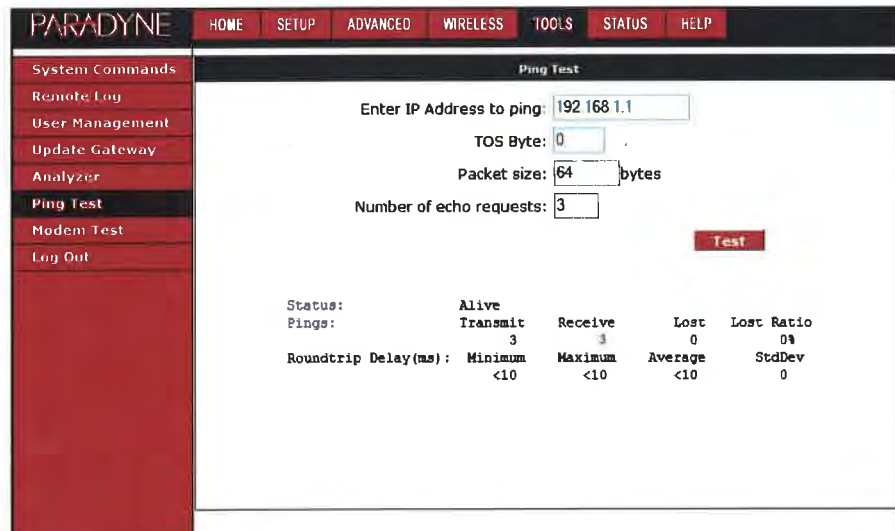


Figure 3-47. Ping Test

Modem Test

The Modem Test is used to check whether your router is properly connected to the WAN Network by running OAM F4 and F5 end-to-end and segment tests. The test may take a few seconds to complete. To perform the test, select your connection from the list, select a Test Type, and click on the Test button.

Before running this test, make sure you have a valid DSL link; if the DSL link is not connected, this test will always fail. Also, the DSLAM must support this feature. Not all DSLAMs have OAM F4 and F5 support.

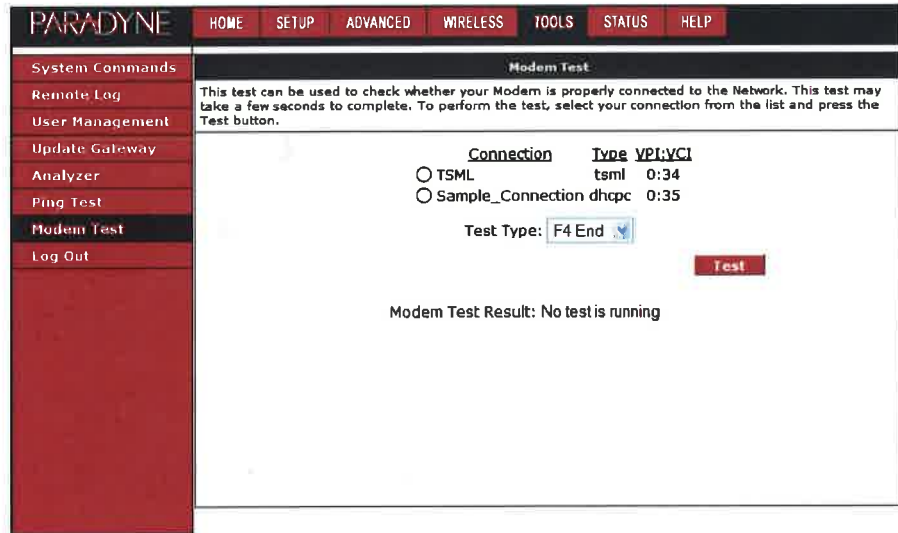


Figure 3-48. Modem Test

Status

The Status section allows you to view the Status/Statistics of different connections and interfaces:

- Network Statistics – Select to view the Statistics of the Ethernet and DSL interfaces, as shown in [Figure 3-49](#).

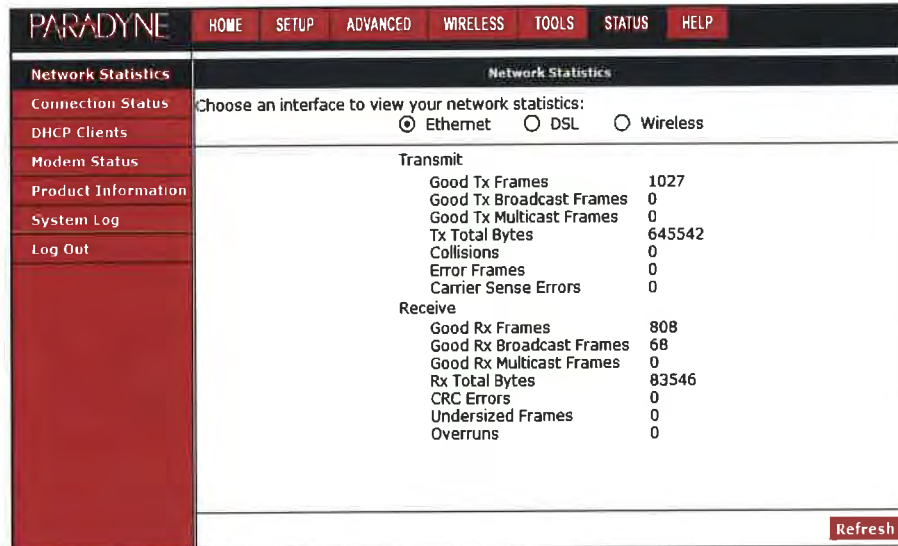


Figure 3-49. Network Statistics

- Connection Status – Select to view the Status of different connections.
- DHCP Clients – Select to view the list of DHCP clients.
- Modem Status – Select to view the Status and Statistics of your broadband (DSL) connection, as shown in [Figure 3-50](#).

Modem Status	
Connection Status	Connected
Us Rate (Kbps)	960
Ds Rate (Kbps)	8128
US Margin	6
DS Margin	15
Trained Modulation	T1413
LOS Errors	0
DS Line Attenuation	0
US Line Attenuation	0
Peak Cell Rate	2264 cells per sec
CRC Rx Fast	0
CRC Tx Fast	1
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path
DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

Figure 3-50. Modem Status

- Product Information – Select to view the router's driver and run-time information, as shown in [Figure 3-51](#).

Software Version	R3.00.04
DSL Datapump	t030600
Boot Loader	1.2.1.5
Model Number	AR7WRD
HW Revision	Unknown
Serial Number	none
Ethernet MAC	N/A
WAN MAC	N/A
AP MAC	N/A

Figure 3-51. Product Information

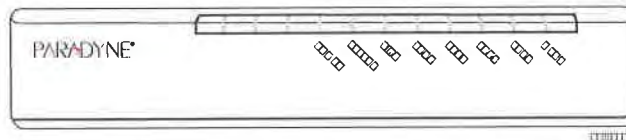
- System Log – Select to view all logged information. Depending upon the severity level, this logged information will generate log reports to a remote host (if remote logging is enabled).

Troubleshooting

4

The Router Is Not Functional

1. Check to see that the power LED is green and that the network cables are installed correctly. Refer to [Connecting the Hardware](#) in Chapter 2, Hardware Installation and PC Setup for more details.
2. Check to see that the LAN and STATUS LEDs are green.
3. Check to see that the STATUS LED is green.



4. Check the settings on your PC. Again, refer to the quick start guide for more details
5. Check the router's settings.
6. From your PC, can you ping the router? Assuming that the router has DHCP enabled and your PC is on the same subnet as the router, you should be able to ping the router.
7. Can you ping the WAN? Your ISP should have provided the IP address of their server. If you can ping the router and your protocols are configured correctly, you should be able to ping the ISP's network. If you cannot ping the ISP's network, make sure you are using the correct protocols with the correct VPI/VCI values.
8. Make sure NAT is enabled if you are using private addresses on the LAN ports.

You Cannot Connect to the Router

1. Check to see that the power LED is green and that the network cables are installed correctly.
2. Make sure that your PC and the router are on the same network segment. The router's default IP address is 192.168.1.1. If you are running a Windows-based

PC, type `ipconfig /all` (or `wiipcfg /all` on Windows 95, 98, or ME) at a command prompt to determine the IP address of your network adapter. Make sure that it is within the same 192.168.1.x subnet. Your PC's subnet mask must match the router's subnet mask. The router has a default subnet mask of 255.255.255.0.

3. Make sure NAT is enabled if you are using private addresses on the LAN ports.

LEDs Blink in a Sequential Pattern

This typically means that either the kernel or flash file system is corrupted. Notify your service representative.

Status LED Continues to Blink

This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The main cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.

Status LED is Always Off

1. Make sure you have DSL service. You should receive notification from your ISP that DSL service is installed. You can usually tell if the service is installed by listening to the phone line: you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.
2. Verify that the phone line is connected directly to the wall and to the line input on the router. If the phone line is connected to the phone side of the router or you have a splitter installed on the phone line, the DSL light will not come on.

Terminology



What is a Firewall?

A firewall is protection between the Internet and your local network. It acts as the firewall in your car does, protecting the interior of the car from the engine. Your car's firewall has very small opening that allow desired connections from the engine into the cabin (gas pedal connection, etc), but if something happens to your engine, you are protected.

The firewall in the router is very similar. Only the connections that you allow are passed through the firewall. These connections normally originate from the local network, such as users web browsing, checking e-mail, downloading files, and playing games. However, you can allow incoming connections so that you can run programs like a web server.

What is NAT?

NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address to access the Internet with. However, you may have several machines on your local network that want to access the Internet at the same time. The router provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine.

Occasionally, there are certain programs that don't work well through NAT. Some games and other specialty applications have a bit of trouble. The router contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a server. See the DMZ section below.

What is a DMZ?

DMZ really stands for Demilitarized Zone. It is a way of separating part of your local network so that is more open to the Internet. Suppose that you want to run a web server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to isolate the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.

Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the server's network address to others, you actually provide the address of the router. The router fakes the connection to your machine.

You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers) should not be connected to the DMZ.

What is a Router?

The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.

Index

A

About This Guide, v
Access Control, 3-37
ADSL, 1-1
ADSL/R, 1-1
ADSL2+, 1-1
Advanced, 3-23
Advanced Features, 3-23
Analyzer screen, 3-49
Assigning IP Address using DHCP, 2-3

B

Back Panel, 1-2
Bridge, 1-1
 Connection, 3-14
 Filters, 3-30
Bridge Filters, 3-30
Bridged Connection, 3-14

C

Cables
 Installing, 2-1
CE Marking, B
Changing IP address, 3-20
CLIP Connection, 3-15
Configuring
 LAN, 3-19
 PC's IP Address, 2-3
 WAN, 3-6
Connecting Hardware, 2-1
CPE update feature, 3-25

D

Declaration of Conformity, D
default settings, 1-2
Definitions, 1-1
DHCP
 Connection Setup, 3-12
 Enable/Disable, 3-19
DMZ, Explained, A-1
DoC, D
Document
 Feedback, A
 Purpose and Intended Audience, v
 Summary, v

duplex mode, 3-21
Dynamic Routing, 3-35

E

EMI Notice
 Canada, D
 Japan, D
Enable/Disable DHCP, 3-19
ending session, 3-37
end-to-end test, 3-51
Ethernet
 cable, 2-1
 switch configuration, 3-21

F

factory default settings, 1-2
FCC Part 15 Declaration, B
Features of the Router, 1-1
filters
 bridge, 3-30
 IP, 3-28
 web, 3-32
Firewall
 Enabling, 3-22
 Explained, A-1
Firewall/NAT Services, 3-22
Firmware Upgrade, 3-48

H

Hardware Installation, 2-1
Home Page, 3-2

I

ICMP echo request, 3-50
IGMP, 3-33
IGMP Snooping, 3-34
Important Safety Instructions, B
Introduction, 1-1
IP Address
 assigning by DHCP, 2-3
 of PC, 2-3
 of Router, 3-20
 Static, 3-11
 trap upon change, 3-25
IP Filters, 3-28

IP QoS, 3-26

J

Japan Notices, D

L

LAN

- Clients, 3-29
- Configuring, 3-19
- Connection, 3-5
- LED, 1-3
- ports, connecting, 2-1

LED

- Blinking in a Sequential Pattern, 4-2
- Description, 1-2
- Link, 1-3
- Status LED continues to blink, 4-2

Link LED, 1-3

Local Area Network Connection, 3-5

Logging In, 3-1

Logging Out, 3-37

M

Management link (TSML), 3-18

Modem

- Setup, 3-17
- Test, 3-51

Modify Existing Connection, 3-16

Modulation Type, 3-17

Multicast, 3-33

N

NAT

- explained, A-1
- Service, 3-22

Network Interface Card, 2-1

New Connection, 3-7

NOC access, 3-18

Notice

- to Users of the Canadian Telephone Network, D
- to Users of the United States Telephone Network, C

O

OAM F4 and F5 tests, 3-51

Overview, 2-1

P

packet size, 3-50

Packing List, 1-3

Password, 3-1

PC Setup, 2-1

Ping Test, 3-50

Port Forwarding, 3-26

port speed, 3-21

Ports and Buttons (Back Panel), 1-2

Power LED, 1-2

power supply, 2-1

PPPoA

- Connection Setup, 3-9

PPPoE

- Connection Setup, 3-7
- Support, 1-2

Product-Related Documents, v

PVC Support, 1-2

Q

QoS, 3-26

Quality of Service, 3-26

Quick Start Options, 3-4

R

ReachDSL, 1-1

Remote Logging, 3-45

Requirements, 1-2

Reset Button, 1-2

Router, 1-1

Routing

- Dynamic, 3-35
- Static, 3-34

S

Saving Changes, 3-5

segment test, 3-51

Setup, 3-5

Severity Levels, 3-46

Simple Network Management Protocol, 3-25

Simple Network Time Protocol, 3-24

SNMP, 3-25

SNTP, 3-24

speed of LAN port, 3-21

Static

- Connection Setup, 3-11
- Routing, 3-34

Status, 3-52

LED, 1-2

LED always off, 4-2

LED continues to blink, 4-2

Supplier's Declaration of Conformity, D

switch configuration, 3-21

System

- Commands, 3-45
- Requirements, 1-2

T

Terminology, A-1

Tests

OAM F4 and F5, 3-51

Ping, 3-50
results, 3-49

Tools, 3-45

TOS byte, 3-50

Trademarks, A

Traps, 3-25

Troubleshooting, 4-1

Troubleshooting Management Link, 3-18

TSML, 3-18

U

Update Gateway, 3-48

Upgrade Firmware, 3-48

UPnP, 3-23

User Management, 3-47

Username, 3-1

V

VLAN, 3-29

W

WAN

Configuring, 3-6

Connection, 3-5

Warranty, Sales, Service, and Training Information, A

Web filters, 3-32

Web Interface, using, 3-1

Wide Area Network Connection, 3-5

Windows

2000, 2-5

95, 98, 2-7

ME, 2-6

NT 4.0, 2-8

XP, 2-3

DSL Forum



Approved Technical Reports

Recently Approved TR's

[[TR-090](#): Protocol Independent Object Model for Managing Next Generation ADSL Technologies]

DSL-Related Standards and References

Report Number	Title (Word File)	PDF File	Date	Working Group	Former Working Text Number	Additional Information	Status: Active=A Obsolete=O
TR-001	ADSL Forum System Reference Model	PDF	May 1996	All	WT-001		A
TR-002	ATM over ADSL Recommendations	PDF	Mar 1997	ATM End-to-End	WT-006	Superseded by TR-017	O
TR-003	Framing and Encapsulation Standards for ADSL: Packet Mode	PDF	Sep 1997	Packet Mode	WT-004		A
TR-004	Network Migration	PDF	Dec 1997	Network Mgmt	WT-013		A
TR-005	ADSL Network Element Management	PDF	Mar 1998	Network Mgmt	WT-008		A
TR-006	SNMP-based ADSL LINE MIB	PDF	Mar 1998	Network Mgmt	WT-015	Superseded by TR-027	O
TR-007	Interfaces and System Configurations for ADSL: Customer Premises	PDF	Mar 1998	Customer Premises	WT-011		A
TR-008	Default VPI/VCI addresses for FUNI Mode Transport: Packet Mode	PDF	Mar 1998	Packet Mode	WT-016	Intended to complete paragraph 3.1.2 of TR-003, entitled "Address Assignment"	A
TR-009	Channelization for DMT and CAP ADSL Line Codes: Packet Mode	PDF	Mar 1998	Packet Mode	WT-017		A
TR-010	Requirements and Reference Models for ADSL Access	PDF	Mar 1998	SNAG	WT-014		A

EXHIBIT A

	Networks: The "SNAG" Document						
TR-011	An End-to-End Packet Mode Architecture with Tunneling and Service Selection	PDF	Jun 1998	Packet Mode	WT-019		A
TR-012	Broadband Service Architecture for Access to Legacy Data Networks over ADSL ("PPP over ATM")	PDF	Jun 1998	ATM End-to-End	WT-020v2		A
TR-013	Interface & Configurations for ADSL: Central Office	PDF	Mar 1999	CPE & CO	WT-018v5		A
TR-014	DMT Line Code Specific MIB	PDF	Mar 1999	Network Mgmt & Operations	WT-022v4	Superceded by TR-024	O
TR-015	CAP Line Code Specific MIB	PDF	Mar 1999	Network Mgmt & Operations	WT-023v4	Definitions supplement the IETF ADSL line MIB, which was derived from TR-006	A
TR-016	CMIP-based Network Management Framework	PDF	Mar 1999	Network Mgmt & Operations	WT-025v4	Superceded by TR-028	O
TR-017	ATM over ADSL Recommendation and (TR-017 Annex)	PDF	Mar 1999	ATM End-to-End	WT-025v4	Superceded by TR-042	O
TR-018	References and Requirements for CPE Architectures for Data Access	PDF	May 1999	ATM End-to-End	WT-031v3		A
TR-019	ADSL Forum Recommendation for Physical Layer of ADSLs with a Splitter	PDF	May 1999	All	PR-001		A
TR-020	ADSL Forum Recommendation for Physical Layer of ADSLs without a Splitter	PDF	May 1999	All	PR-002		A
TR-021	ADSL Forum Recommendation for ATM layer of ADSLs	PDF	May 1999	All	PR-003		A
TR-022	The Operation of ADSL-based	PDF	Aug 1999	Network Mgmt & Operations	WT-026v6		A

EXHIBIT A

	<u>Networks</u>						
TR-023	Overview of ADSL Testing	PDF	Aug 1999	Testing & Interoperability	WT-027v5		A
TR-024	DMT Line Code Specific MIB	PDF	Aug 1999	Network Mgmt & Operations	WT-036v2	Updated version of TR-014	A
TR-025	Core Network Architecture for Access to Legacy Data Network over ADSL	PDF	Nov 1999	ATM End-to-End	WT-033v5		A
TR-026	T1.413 Issue 2, ATM-based ADSL ICS	PDF	Nov 1999	Testing & Interoperability	WT-034v5		A
TR-027	SNMP-based ADSL LINE MIB	PDF	Nov 1999	Network Mgmt & Operations	WT-037v3	Updated version of TR-006	A
TR-028	CMIP Specification for ADSL Network Element Management	PDF	Dec 1999	Network Mgmt & Operations	WT-037v3	Updated version of TR-016	A
TR-029	ADSL Dynamic Interoperability Testing	PDF	Feb 2000	Testing & Interoperability	WT-029v7		A
TR-030	ADSL EMS to NMS Functional Requirements	PDF	Feb 2000	Network Mgmt & Operations	WT-041v1		A
TR-031	ADSL ANSI T1.413 - 2001 Conformance Testing	PDF	May 2000	Testing & Interoperability	WT-28v9		A
TR-032	CPE Architecture Recommendations for Access to Legacy Data Networks	PDF	May 2000	ATM Mode	WT-032v5		A
TR-033	ITU-T G.992.2 (G.lite) ICS	PDF	May 2000	Testing & Interoperability	WT-035v6		A
TR-034	Proposal for an Alternative OAM Communications Channel Across the U Interface	PDF	May 2000	Network Mgmt & Operations	WT-040v3		A
TR-035	Protocol Independent Object Model for ADSL EMS-NMS Interface	PDF	May 2000	Network Mgmt & Operations	WT-045v2		A
TR-036	Requirements for Voice over DSL	PDF	Aug 2000	VoDSL	WT-043v5	Superceded by TR-039	O

EXHIBIT A

TR-037	Network Management & Operations: DSL CPE Auto-Configuration	PDF	Mar 2001	Operations & Network Management	WT-048v5		A
TR-038	DSL Service Flow-Thru Management Overview	PDF	Mar 2001	Operations & Network Management	WT-050v5	Superseded by TR-054	O
TR-039	Addendum to TR-036 Annex A: Requirements for Voice over DSL	PDF	Mar 2001	VoDSL	WT-055v1	Updated version of TR-036	A
TR-040	Aspects of VDSL Evolution	PDF	Jun 2001	Emerging DSLs	WT-047v8		A
TR-041	CORBA Specification for ADSL EMS-NMS Interface	PDF	Jun 2001	Operations & Network Management	WT-046v5		A
TR-042	ATM Transport over ADSL Recommendation (Update To TR-017)	PDF	Aug 2001	ATM	WT-049v6	Updated version of TR-0017	A
TR-043	Protocols at the U Interface for Accessing Data Networks using ATM/DSL	PDF	Aug 2001	ATM	WT-053v5		A
TR-044	Auto-Configuration for Basic Internet (IP-based) Services	PDF	Nov 2001	Auto-Configuration	WT-059v5		A
TR-045	PPP Static Interoperability Testing	PDF	February 2002	Testing & Interoperability	WT-052v8		A
TR-046	Auto-Configuration: Architecture & Framework	PDF	February 2002	Auto-Configuration	WT-060v4		A
TR-047	DSL Service Flow-Through Fulfillment Management Interface	PDF	February 2002	Operations and Network Management	WT-063v4		A
TR-048	ADSL Interoperability Test Plan	PDF	April 2002	Testing & Interoperability	WT-062v9		O
TR-049	VoDSL Interoperability Test Plan	PDF	May 2002	Testing & Interoperability	WT-066v4		A
TR-050	CORBA v2 for ADSL EMS-NMS Interface	PDF	May 2002	Operations & Network	WT-069v3		A

EXHIBIT A

				Management			
TR-051	DSL Specific Conventions for the ITU-T Q.822.1 Performance Management Bulk Data File Structure	PDF	May 2002	Operations & Network Management	WT-070v3		A
TR-052	DSL Service Flow-Through Fulfillment Management Interface Addendum (DSL Anywhere)	PDF	August 2002	Operations & Network Management	WT-071v2	Supplementing TR-047	A
TR-053	DSL Service Flow-Through Senarios	PDF	August 2002	Operations & Network Management	WT-073v1		A
TR-054	DSL Service Flow-Through Fulfillment Management Overview	PDF	August 2002	Operations & Network Management	WT-074v1	Updates and supercedes TR-038	A
TR-055	ICS for ANSI T1.421 In-line Filters	PDF	February 2003	Testing & Interoperability	WT-067v3		A
TR-056	Network Migration	PDF	February 2003	Architecture & Transport	WT-075v5		A
TR-057	VDSLNetwork Element Management	PDF	February 2003	Operations & Network Management	WT-068v5		A
TR-058	Multi-Service Architecture & Framework Requirements	PDF	September 2003	Architecture & Transport	WT-080v7		A
TR-059	DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services	PDF	September 2003	Architecture & Transport	WT-081v9		A
TR-060v2	Interoperability Test Plan for SHDSL	PDF	November 2003	Testing & Interoperability	WT-079v5		A
TR-061	Interfaces and System Configurations for ADSL: Customer Premises	PDF	November 2003	Architecture & Transport	WT-083v3		A
TR-062	Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT)	PDF	November 2003	Auto-Configuration	WT-088v3		A

EXHIBIT A

	and the Network using ATM (TR-037 update)						
TR-063	Update to TR-057	PDF	November 2003	Operations & Network Management	WT-091v2		A
TR-064	LAN-Side DSL CPE Configuration Specification	PDF	May 2004	DSLHome-Technical	WT-082v9		A
TR-065	FS-VDSL EMS to NMS Interface Functional Requirements	PDF	March 2004	Operations & Network Management	WT-084v5		A
TR-066	ADSL Network Element Management (Update to TR-005)	PDF	March 2004	Operations & Network Management	WT-089v2		A
TR-067	ADSL Interoperability Test Plan (Formerly TR-048)	PDF	May 2004	Testing & Interoperability	WT-085v8		A
TR-068	Base Requirements for an ADSL Modem with Routing	PDF	May 2004	DSLHome-Technical	WT-086v8		A
TR-069	CPE WAN Management Protocol	PDF	May 2004	DSLHome-Technical	WT-087v8		A
TR-070	SCM Specific Managed Objects In VDSL Network Element	PDF	May 2004	Operations & Network Management	WT-096v1		A
TR-090	Protocol Independent Object Model for Managing Next Generation ADSL Technologies	PDF	December 2004	Operations & Network Management	WT-090v5		A
TR-092	Broadband Remote Access Server (BRAS) Requirements Document	PDF	August 2004	Architecture & Transport	WT-092v6		A
TR-094	Multi-Service Delivery Framework for Home Networks	PDF	August 2004	Architecture & Transport and DSLHome Technical	WT-094v4		A

EXHIBIT A

http://web.archive.org/web/20050129232246/http://www.dslforum.org/aboutdsl/Technical_Reports/TR-059.pdf

Technical Report DSL Forum TR-059

DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services

September 2003

**Produced by:
Architecture & Transport Working Group
Editor: Tom Anschutz, BellSouth
Telecommunications**

**Working Group Co-Chair: David Allan, Nortel Networks
Working Group Co-Chair: David Thorne, BT**

Abstract:

This Working Text will outline an evolution of mass market DSL services to deliver multiple levels of QoS enabled IP layer services to DSL subscribers. In support of this service evolution, a reference architecture and supporting requirements are included that outline the interface specifications needed from a subscriber or a Service Provider to access these new services.

Notice:

The DSL Forum is a non-profit corporation organized to create guidelines for DSL network system development and deployment. This Technical Report has been approved by members of the Forum. This document is not

binding on the DSL Forum, any of its members, or any developer or service provider involved in DSL. This document is subject to change, but only with approval of members of the Forum.

©2003, 2004 Digital Subscriber Line Forum. All Rights Reserved.

DSL Forum technical reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only.

Notwithstanding anything to the contrary, the DSL Forum makes no representation or warranty, expressed or implied, concerning this publication, its contents or the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by the DSL Forum as a result of reliance upon any information contained in this publication. The DSL Forum does not assume any responsibility to update or correct any information in this publication.

Revision History	Date	Reason for Update
Version 1	September, 2002	Created new document based on technical requirements sections of dsl2002.213
Version 2	October, 2002	Comments and minor updates from Oct. 8 call
Version 3	December, 2002	Comments and minor updates from Nov. 12 call
Version 4	December, 2002	Comments and updates from December DSLF meeting in San Francisco – except, this version does not yet number requirements – as was agreed.
Version 5	February, 2003	Introduced numbered requirements, removed “RSVP-like,” accepted reviewed changes from V4, and incorporated contributions from January interim teleconference.
Version 6	March, 2003	Moved Phase-2 QoS and Multicast information into Appendix as agreed in February DSLF meeting in Dallas.
Version 7	March, 2003	Collected Interim Meeting Comments (largely editorial) in preparation for straw ballot.
Version 8	May, 2003	This version captures straw ballot comments resolved in Lisbon and is intended to be the text to work from on the Straw ballot comments finalization call.
Version 9	June, 2003	This version captures straw ballot comments resolved in interim meeting and is intended to be the text for letter ballot.
Version 10	February, 2004	This version corrects typographical errors, updates references to WT-080 and WT-081, and improves the PDF and black-and-white output for some figures.

Table of Contents

1	PURPOSE AND SCOPE	1
1.1	PURPOSE	1
1.2	SCOPE.....	1
1.3	REQUIREMENTS.....	2
2	PRODUCTS AND SERVICES.....	2
2.1	SERVICE GOALS	2
2.2	PRODUCT AND SERVICE LISTS	2
3	FUNCTIONAL ASSUMPTIONS.....	4
3.1	KEY TERMINOLOGY.....	4
3.2	BROADBAND PROVIDER REFERENCE DEFINITIONS.....	6
3.3	INTERFACES.....	8
3.3.1	A10-ASP Interface.....	9
3.3.2	A10-NSP Interface.....	9
3.3.3	U Interface.....	9
3.3.4	T Interface.....	9
4	REFERENCE ARCHITECTURE.....	9
4.1	LOGICAL REFERENCE ARCHITECTURE	9
4.2	LOGICAL ELEMENTS AND INTERFACES	11
4.2.1	Application Service Provider Network	11
4.2.2	A10-ASP Interface.....	12
4.2.3	Network Service Provider Network.....	14
4.2.4	A10-NSP interface.....	14
4.2.5	Regional/Access Network.....	18
4.2.6	U Interface.....	22
4.2.7	Customer Premises Network.....	24
4.2.8	T Interface.....	26
5	QUALITY OF SERVICE	28
5.1	INTRODUCTION	28
5.1.1	Goals.....	29
5.1.2	Assumptions	29
5.2	TRAFFIC ENGINEERING OF BEST EFFORT SERVICE	29
5.2.1	Theory of Operation	29
5.3	QoS ARCHITECTURE - A TWO-PHASED APPROACH.....	30
5.3.1	Phase 1 QoS Mechanisms	30
5.3.2	Phase 2 QoS Mechanisms	33
6	SERVICE LEVEL MANAGEMENT.....	36
6.1	INTRODUCTION	36
6.2	NETWORK PERFORMANCE METRICS.....	36
6.3	OPERATIONAL METRICS.....	36
7	SERVICE MANAGEMENT	36
7.1	SUBSCRIBERS.....	37
7.2	SERVICE PROVIDERS	37

GLOSSARY38

APPENDIX A REFERENCES41

APPENDIX B INFORMATIVE EXAMPLE OF QUEUING ARCHITECTURES FOR RG AND BRAS.....42

 B.1 EXAMPLE QUEUING ARCHITECTURE FOR RG42

 B.2 EXAMPLE QUEUING ARCHITECTURE FOR A BRAS THAT CAN ALSO SWITCH ATM43

APPENDIX C INFORMATIVE APPENDIX ON SIGNED QOS.....47

 C.1 SIGNED QOS MECHANISMS47

 C.1.1 Signed QoS Assumptions47

 C.1.2 Diffserv Assumptions48

 C.1.3 Traffic Engineering Requirements48

 C.1.4 Admission Control48

Table of Figures

Figure 1 – DSL Network Components7

Figure 2 – Many-to-Many Access7

Figure 3 – ATM based Regional and Access Network Providers 10

Figure 4 – IP Enabled Regional Network..... 11

Figure 5 – A10-ASP Interface.....12

Figure 6 – ASP Protocol Stack with QoS.....13

Figure 7 – A10-NSP Interface Supporting L2TP Connection 15

Figure 8 – L2TP Protocol Stack..... 15

Figure 9 – A10-NSP Interface Supporting IP Routed Connection 16

Figure 10 – Routed IP Protocol Stack with QoS 17

Figure 11 – Components of the Regional/Access Network 18

Figure 12 – Aggregation function of Regional Network 19

Figure 13 – Access Node Architecture Variations.....22

Figure 14 – U Interface23

Figure 15 – U Interface Protocol Stack24

Figure 16 – T Interface.....27

Figure 17 – IP over Ethernet.....28

Figure 18 – IP over PPP over Ethernet.....28

Figure 19 – Best Effort TE30

Figure 20 – QoS-enabled Network Topology32

Figure 21 – Phase 2 with Policy-based profiles34

Figure 22 – Queuing and Scheduling Example for RG.....43

Figure 23 – Reference Topology for Queuing and Scheduling Example for a BRAS that can also switch ATM.44

Figure 24 – Queuing and Scheduling Example for a BRAS that can also switch ATM46

1 PURPOSE AND SCOPE

1.1 Purpose

ADSL service providers are highly interested in advancing DSL to be the preferred broadband access technology by growing their networks, increasing the value provided by those networks, and expanding the market they can address. To do this they must address several critical needs, particularly:

- The service must become more accessible to end-users and to wholesale and retail partners.
- The service must address a wider market with:
 - Variable speeds,
 - Variable precedence arrangements – allowing some application's traffic to take precedence over others.
 - Specific support for IP applications (e.g. IP-QoS and multicasting),
 - Support for new business models that can include more types of service providers, and
 - Support for these new service parameters across multiple connections to different service providers from a single DSL subscriber.
- The service must be competitive with alternative access technologies such as cable modem.

While adopting new architectures, like FSVDSL, may also fulfill these needs, perhaps even better than the architecture defined here, it is also important to realize that much ADSL has already been deployed, and that the current business imperatives may cause ADSL service providers to try to make more of what they already have than to try massive upgrades along with the massive capital investment they usually bring.

Therefore, there is also a critical need to provide a standard evolution path for the embedded base of ADSL.

The purpose of this work and the new service models is to provide a more common architecture and set of service interfaces to address these critical needs. Adhering to this architecture and to the services and service models set forth both here and in TR-058 simplifies and unifies the way for all types of service providers to obtain ADSL end-user customers whether they sell access to networks, applications, or content.

The anticipated outcome for employing this specification, as well as others that build from it, is that it will:

- Reduce the number of alternative interfaces to ISPs/ASP and end users, in order to reduce costs through common interconnection.
- Establish guidelines for developers and vendors, so they can build equipment that support common service requirements.
- Improve the ability to introduce end-to-end services and applications worldwide, so that similar services can interwork across various service providers' networks.

1.2 Scope

This document presents an architecture for evolving DSL deployment and interconnection including the LAA and PTA architectures defined in TR-25. It outlines a common methodology for delivering QoS-enabled applications to DSL subscribers from one or more Service Providers. The business framework and drivers justifying this architectural evolution are described, in part, in TR-058. In the largest sense, the scope of this architecture is to provide IP-QoS and more flexible service arrangements to millions of users and thousands of service providers. And to do this to a useful extent, while pursuing only economic enhancements to existing ADSL networks.

While ADSL is useful for mass markets, segments and niches – this architecture addresses the mass market specifically. The approach, service models, and architecture are intended to scale to thousands of service providers, and many millions of end-users. The architecture does not detail approaches and techniques that might be appropriate to segments and niches, but does recognize that they might also be used in concert with

this approach. Similarly, local regulations, e.g. wiretapping, might apply to this and any architecture, but are beyond the scope of this document.

Many of the requirements levied on network elements and management systems are collected in this architecture, but they should not be taken as an exhaustive list of requirements for such elements. It is expected that other documents and standards will come forward to collect the requirements here, as well as those from other markets, segments, and niches in order to provide complete requirements for elements and systems that wish to be suitable in the DSL industry.

This architecture provides a high-level, evolving view of ADSL access. Because of this it provides more details about things that will happen sooner and fewer details about things that are several years and phases from fruition. Also, unlike a design, this architecture does not provide exhaustive instructions on how to develop and deploy networks or elements that adhere to the architecture. In fact, it identifies the need to develop and standardize new functions, features, and protocols in many later-phase areas.

1.3 Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized.

- | | |
|-----------------|---|
| MUST | This word, or the adjective "REQUIRED", means that the definition is an absolute requirement of the specification |
| MUST NOT | This phrase means that the definition is an absolute prohibition of the specification. |
| SHOULD | This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course. |
| MAY | This word, or the adjective "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option MUST be prepared to inter-operate with another implementation that does include the option. |

2 PRODUCTS AND SERVICES

2.1 Service Goals

Despite efforts to unify the architecture of Service Provider connections and to provide common service tiers, there has not been general support for a unified architecture. This proposal intends to increase the interest in such an architecture by increasing the number of service parameters available as well as by making those parameters more dynamic. Aside from variable dynamic bandwidth, this new architecture includes Quality of Service (QoS) and multi-application/multi-destination selection.

Service Providers benefit in that they will only need to develop one set of system interfaces for any carrier that adopts this architecture. By subscribing to these interfaces, Service Providers will now be able to develop applications that can take advantage of variable bandwidth and differentiated data traffic delivery that supports better than *best effort* traffic classes. Subscribers will be able to realize greater potential of their broadband data connections. This means that a subscriber can still use their Internet access as it exists today; yet additional bandwidth on their DSL line can be used to deliver other applications, such as direct corporate access, video chat and video conferencing, and various content on demand - be it movies, games, software, or time-shifted television programs. Finally, these applications can be given QoS treatment, so that business access, online gaming, and casual Internet access all share bandwidth appropriately. Both subscribers and Service Providers will be able to choose who provides the best service for a specific application, and what applications add the most value.

2.2 Product and Service Lists

This document presents a proposal for evolving DSL deployment and interconnection. It will outline a common methodology for delivering QoS-enabled applications to DSL subscribers from multiple Service Providers. These products and services are intended to address the mass market, and do not preclude additional niche or custom services that could be provided using the same infrastructure. Many of the current products offered

today either can be adapted to contain or already do contain the necessary software needed to support the proposed architectures contained within this document.

Also provided is a set of architectural requirements to support the proposed new service models. Some of the highlights include:

- IP-based services and QoS
- A single network control plane
- The migration of DSL regional transport to leverage newer, alternative technologies

The prevalent existing service model, where subscriber connections are delivered in a best effort fashion over end-to-end ATM PVCs, will continue to exist. However, this service model cannot support many of the improvements and benefits desired, including IP QoS, bandwidth on demand, and utilization of newer, alternative transport options.

This architecture supports the following service provider interconnection models, which are described TR-058:

- Subscriber access using PPPoE aggregated into L2TP tunnels delivered to Network Service Providers.
- Subscriber access using PPPoE or IP over Ethernet aggregated into VPNs delivered to Network Service Providers.
- Subscriber access using PPPoE or IP over Ethernet aggregated into a common, public, QoS-enabled IP network and delivered to Application Service Providers.

The DSL architecture and requirements put forward by this document enable the following product and service enhancements, which are described in TR-058.

- Bandwidth on Demand
- QoS, including QoS on Demand
- Many-to-Many Access
- Content Distribution

Network Service Providers will be able to benefit from the aggregation capabilities of the new DSL Access Networks described in this document. Specifically, this architecture will also permit:

- **Traffic Aggregation:** The end-to-end ATM PVC models, whether VPC or VCC, do not provide a scalable solution. L2TP and IP are used to provide better scalability and efficiency.
- **Improved Transport:** Currently most DSL transport is done over ATM connections. By offering other transport options, like Packet over SONET (POS) and Metro Ethernet, this architecture can provide better scalability, reduced overhead, and increased flexibility.
- **Simpler Provisioning:** Because they are not directly linked to provisioning transport, L2TP and IP delivery models can reduce the level of per subscriber provisioning.
- **Differentiated Services:** Up until now, almost all DSL transport has been best effort delivery. This new IP based architecture will permit Service Providers to offer differentiated treatment for certain traffic.
- **Bandwidth Services:** Up until now, most DSL access has been at a fixed rate that was selected at the time an access was provisioned. This architecture provides mechanisms that allow rates to be selected or changed more often and potentially on-the-fly.

- **Increased Access:** In previous architectures, Service Providers could only reach those subscribers with whom they had a direct relationship. These new architectures permit a subscriber to connect simultaneously to multiple Service Providers for a variety of services. Service Providers no longer need to be the sole provider to their subscribers.
- **Standard Connections:** Up until now, each access provider has had their own set of interfaces for Service Providers. This proposal defines common interfaces for NSPs and ASPs. This means that the Service Provider need only develop a single interface to get all of these features for many access providers. Also, subscriber connections will be similar among Access Providers, allowing common CPE to be more widely deployed.

Support for these new services will require a new set of network management interfaces. Both Service Providers and Subscribers will use these interfaces. Service Providers will be able to examine the network and see how their subscribers are provisioned. NSPs will also be provided an interface to control and troubleshoot subscriber connections.

Subscribers will be provided mechanisms for requesting these new services and indicating specific needs. These requirements will support applications and services like:

- Multicast audio and video media applications
- Video on demand applications
- Voice services
- Interactive gaming
- Variable bandwidth, both on demand ("Turbo" button) and by application

3 FUNCTIONAL ASSUMPTIONS

3.1 Key Terminology

The following definitions apply for the purposes of this document:

Access Network

The Access Network encompasses the elements of the DSL network from the NID at the customer premises to the BRAS. This network typically includes one or more types of Access Node and often an ATM switching function to aggregate them.

Access Node

The Access Node contains the ATU-C, which terminates the DSL signal, and physically can be a DSLAM, Next Generation DLC (NG-DLC), or a Remote Access Multiplexer (RAM). A DSLAM hub can be used in a central office to aggregate traffic from multiple remote physical devices, and is considered logically to be a part of the Access Node. When the term "DSLAM" is used in this document, it is intended to very specifically refer to a DSLAM, and not the more generic Access Node. The Access Node provides aggregation capabilities between the Access Network and the Regional Network. It is the first point in the network where traffic on multiple DSL lines will be aggregated onto a single network.

Behavior

The externally observable characteristic applied to a traffic stream by a network element or system, for example assuring a minimum rate for a video stream or PPP session.

Broadband Remote Access Server (BRAS)

The BRAS is the aggregation point for the subscriber traffic. It provides aggregation capabilities (e.g. IP, PPP, ATM) between the Regional/Access Network and the NSP or ASP. Beyond

	aggregation, it is also the injection point for policy management and IP QoS in the Regional/Access Networks.
Core Network	The center core of the Regional Network. The functions contained herein are primarily transport oriented with associated switching or routing capabilities enabling the proper distribution of the data traffic.
Downstream	The direction of transmission from the Access Node to the DSL modem.
Dropping	The process of discarding packets/cells based on specified rules, which may be the result of for example, a policing action or policy decision.
Edge Network	The edge of the Regional Network. The Edge Network provides access to various layer 2 services and connects to the Regional Network core enabling the distribution of the data traffic between various edge devices.
Layer 2 Tunnel Switch (L2TS)	The L2TS provides a second layer of PPP aggregation beyond the L2TP Access Concentrator (LAC). PPP sessions are switched between L2TP tunnels and are further aggregated and delivered to the NSP.
Loop	A metallic pair of wires running from the customer's premises to the Access Node.
Many-to-Many Access Sessions	The ability for multiple individual users or subscribers, within a single premises, to simultaneously connect to multiple NSPs and ASPs.
Microflow	A single instance of an application-to-application flow of packets, which may for example be classified by source address, source port, destination address, destination port and protocol id, or stateful means.
PVC Bundle	Two or more ATM PVCs (called a "bundle") are co-terminated on router endpoints. Each bundle co-termination is bound to a single IP interface. That is, the two (or more) PVCs appear to be a single "link layer" to the IP layer and so share a single set of routes. DiffServ, TOS marking, or other IP QoS mechanisms are used to select which of the two or more PVCs to use in either direction. Currently PVC bundles apply only to routed, not bridged interfaces. For them to be useful to this architecture, the approach would need to support bridged interfaces in addition to routed interfaces, and would need support simultaneous transport of both PPPoE and IP over one of the PVCs in the bundle.
Regional Network	The Regional Network interconnects between the Network Service Provider's network and the Access Network. A Regional Network for DSL connects to the BRAS, which is technically both in the Regional Network and in an Access Network. Typically more than once Access Network is connected to a common Regional Network. The function of the Regional Network in this document goes beyond traditional transport, and may include aggregation, routing, and switching.
Regional/Access Network	The Regional and Access Networks – grouped as an end-to-end QoS domain and often managed by a single provider.
Routing Gateway	A customer premises functional element that provides IP routing and QoS capabilities. It may be integrated into or be separate from the modem.

Session	A logically identifiable relationship formed between two (or more) communicating entities for exchanging control and data packets. An example of which would be a PPP session.
Subscriber	The client that is purchasing the DSL circuit from the Service Provider and is receiving the billing.
Traffic Classification	The process of selecting packets based on common criteria, such as the content of packet headers or session identification.
Traffic Marking	The process of setting packet header fields, such as DSCP, MPLS EXP or 802.1p/q COS field in a packet/frame/cell based on defined rules. Traffic marking may result from for example, a classification decision, a policing action, or a policy decision.
Traffic Metering	The process of measuring the rate and/or burst of a traffic stream selected by a classifier. The instantaneous state of this process may be used to affect the operation of a marker, shaper, or policer, and/or may be used for accounting and measurement purposes.
Traffic Policing	The process of dropping, marking or remarking packets/cells within a traffic stream in accordance with the state of a corresponding meter against a defined traffic profile, using mechanisms such as the token bucket scheme defined by [RFC2697].
Traffic Remarking	The process of changing header fields, such as DSCP, MPLS EXP or 802.1p/q COS field in a packet/frame based on defined rules.
Traffic Shaping	The process of delaying packets/cells within a traffic stream to cause it to conform to some defined traffic profile.
Traffic Stream	a set of one or more microflows or sessions, which are selected by a particular classifier.
Upstream	The direction of transmission from the modem to the Access Node.
User	Typically, a member, employee or guest at the Subscriber's household or business using the DSL circuit capabilities.

3.2 Broadband Provider Reference Definitions

Generally, services over a DSL access-based broadband network will be provided and supported by a number of different operational organizations. These organizations may be part of one company or more than one company and it is desirable to have a clear idea of the roles of the different organizations and how the functionality of equipment, network management, and test equipment can support their ability to discharge their roles for the benefit of the end customers. In order to provide a baseline with which to contrast, this document provides a common architectural view of DSL architecture in Figure 1.

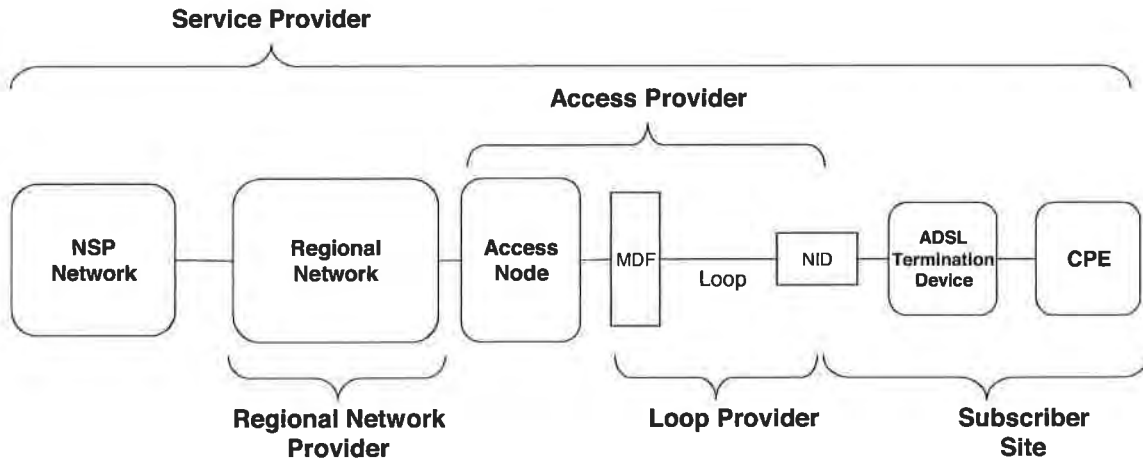


Figure 1 – DSL Network Components
(Voice components not shown for clarity)

Boxes in the figures represent functional entities – networks and logical components rather than physical elements.

This traditional architecture is centered on providing service to a line or a loop. It is desired, however, to be able to provide services that are user-specific. Additionally, more than one subscriber can be present at the same premises and share a single loop. There is a need, therefore, to describe a slightly more complex situation, and hiding the common complexity shared with Figure 1, this description is provided in Figure 2 below. Note that the figure shows many-to-many access through a common Regional/Access network. It is used to simultaneously provide an Application Service₁ between an ASP Network₁ and User₁ at the same time and over the same U interface as it supports a Network Service₂ between NSP Network₂ and User₂.

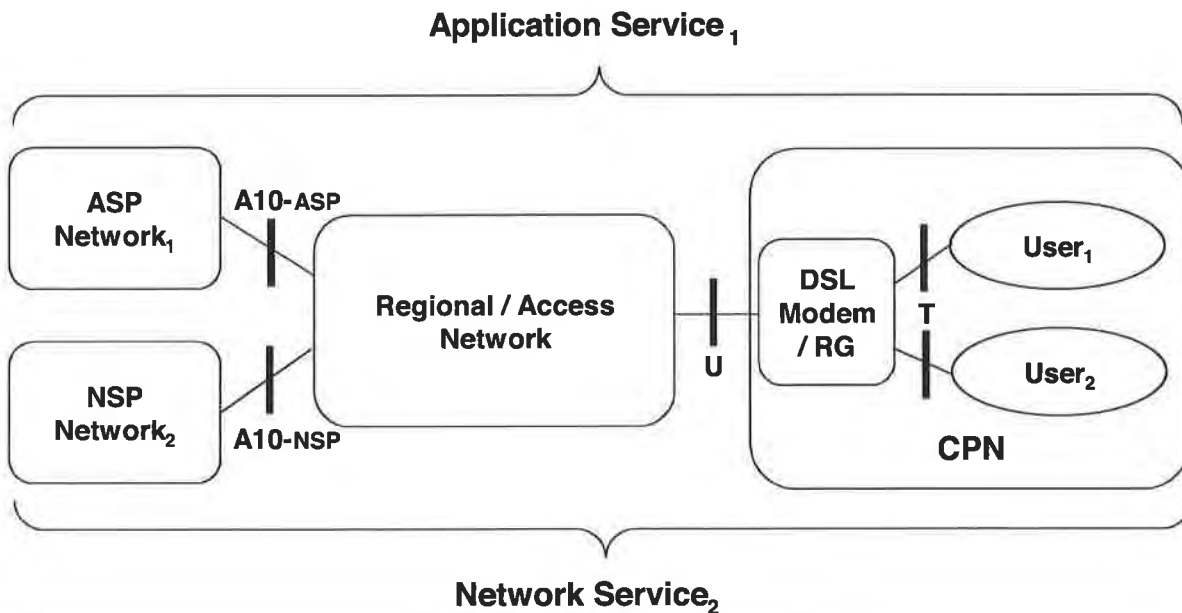


Figure 2 – Many-to-Many Access

The figures show the key components of a DSL access-based broadband network. They indicate ownership of the components to different providing organizations. The role of these various providers is indicated below:

The Network Service Provider (NSP):

- Includes Internet Service Providers (ISPs) and Corporate Service Providers (CSPs)
- Is responsible for overall service assurance
- May provide CPE, or software to run on customer-owned CPE, to support a given service
- Provides the customer contact point for any and all customer related problems related to the provision of this service
- Authenticates access and provides and manages the IP address to the subscribers

The Application Service Provider (ASP):

- Provides application services to the application subscriber (gaming, video, content on demand, IP Telephony, etc.)
- Is responsible for the service assurance relating to this application service
- Responsible for providing to subscribers additional software or CPE which specific services may require.
- Provides the subscriber contact point for all subscriber problems related to the provision of specific service applications and any related subscriber software.
- Does not provide or manage the IP address to the subscribers

The Loop Provider:

- Provides a metallic loop from the Access Network equipment to the customer's premises
- Is responsible for the integrity of the metallic loop and its repair
- May also provide the Access Network Provider aggregated access to remotely deployed DSL equipment owned, operated, and maintained by the Loop Provider

The Access Network Provider:

- Provides digital connectivity to the customer via the metallic Loop
- Is responsible for the performance and repair of the access transmission equipment

The Regional Network Provider:

- Provides appropriate connectivity between the Access Network and the NSPs and ASPs
- Is responsible for Regional Network performance and repair
- May perform aggregation services to NSPs or ASPs and/or may provide any to any connectivity within the RBN on behalf of the NSP/ASP.

3.3 Interfaces

These interfaces are key to this architecture, and have been modified or expanded from historical architectures (except the U interface) and represent requirements specific to the service models detailed herein and in TR-058.

3.3.1 A10-ASP Interface

This reference point is between the Regional/Access Network and the ASP's Points of Presence (POPs). This interface will consist of a routed IP interface, that may be transported over Fast Ethernet, Gigabit Ethernet, Packet over SONET (POS), or some other IP interface. The ASP has the end-to-end Service responsibility to the customer for their specific application and is viewed as the "Retailer" of the specific service. Trouble reports for the specific service go directly to the ASP.

3.3.2 A10-NSP Interface

This reference point is between the Regional/Access Network and the NSP's POPs. The interfaces could be ATM, Fast Ethernet, Gigabit Ethernet, or Packet over SONET (POS). In the case of ATM, multiple PPP sessions may be multiplexed over a single VCC at this interface. Typically, the NSP has the end-to-end service responsibility to the customer and is viewed as the "Retailer" of the service. As the retailer of the DSL service, trouble reports, and other issues from the subscriber are typically addressed to the NSP. Handoff protocols could include layer 2 (e.g. ATM VP/VCs, L2TP tunnels) and layer 3 (e.g. IPv4, IPv6 routed protocols).

3.3.3 U Interface

The U Interface is located at the subscriber premise between the Access Node and the DSL modem.

3.3.4 T Interface

The T Interface defines the interworking between the DSL modem/ Routing Gateway and other CPE in the Customer Premises Network (CPN). The requirements for new vertical services over DSL require the addition of a Routing Gateway as the intermediate point between the DSL modem and the LAN Devices. The primary goal of this interface is to facilitate seamless transmission of IP packets in both a best effort approach as well as maintaining predefined QoS behavior or establishing dynamic QoS behaviors through a signaling mechanism. The DSL modem and Routing Gateway functions may or may not be combined in a single device.

4 REFERENCE ARCHITECTURE

4.1 Logical Reference Architecture

As noted in Section 3.2 above, the end-to-end DSL network consists of four providers. Of these providers, the two that this proposal most affects are the Regional Network Provider and the Access Network Provider. Historically the Regional Network has been a network of ATM switches, as shown in Figure 3. This is because the access to most Access Nodes is an ATM based interface. Some Access Networks even have their own ATM switches used to aggregate traffic from multiple Access Nodes.

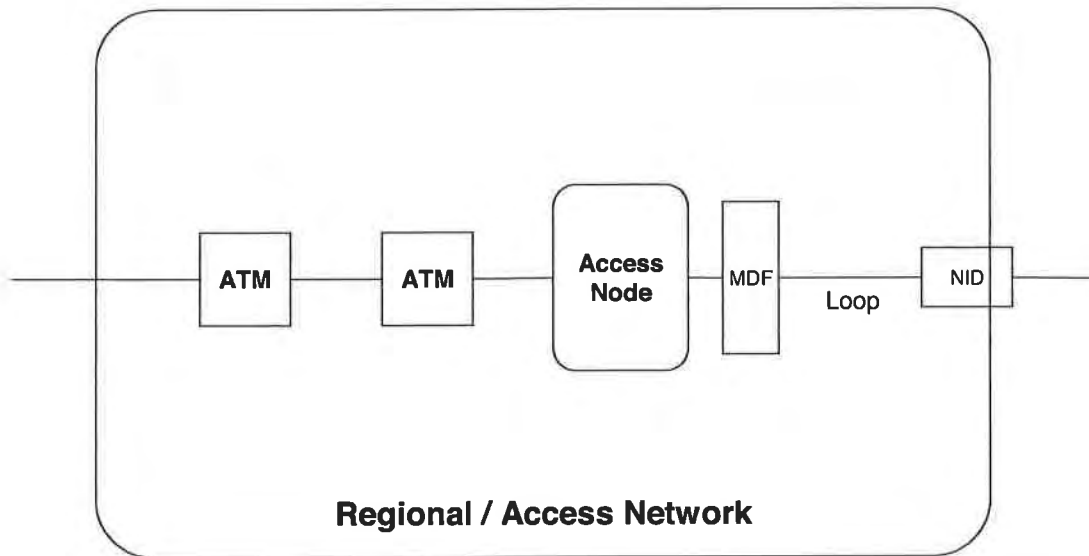


Figure 3 – ATM based Regional and Access Network Providers

In this architecture, there are no mechanisms for limiting subscriber traffic except for per line profiles within the Access Nodes. As many DSL networks were deployed before the advent of the BRAS, almost all the Access Network Providers use fixed speed profiles in the Access Nodes to limit upstream and downstream traffic. Even if the Service Provider were to attempt to send more traffic into the Regional Network than the Access Node is set to permit, the Access Node will police the downstream traffic. Since most Internet-based applications use TCP as the transport protocol, the traffic rejected at the Access Node will trigger TCP back-off, effectively throttling the downstream bandwidth. As such, most Service Providers also shape downstream traffic at the subscriber-selected bandwidth. However, the desire to move to a rate adaptive bandwidth model means that both the Regional and Access Networks could be vulnerable to traffic overloading. A means to control upstream and downstream traffic is needed as this architecture evolves.

Many times the physical components of the Access Nodes are daisy-chained, sharing the bandwidth of the aggregating circuit. As shown in Figure 13 in Section 4.2.5.4, there are numerous ways that DSL access devices can be interconnected to the first ATM switch. While historical measurements have shown that the typical DSL subscriber uses no more than a small fraction of sustained bandwidth, the fact is that as subscribers are offered more and more high bandwidth applications, the average sustained bandwidth per subscriber over these "mid-mile" connections is going to increase. As per subscriber bandwidth usage increases, the Regional Network Provider will also need to scale bandwidth and provide subscriber-level granularity. ATM VPs do not provide the granularity necessary to offer per application QoS on a per subscriber basis.

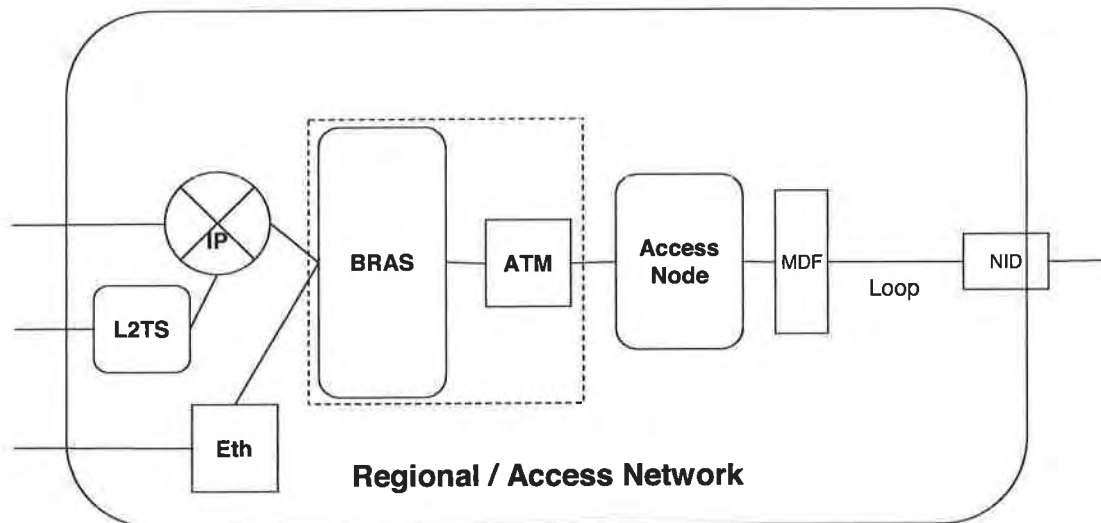


Figure 4 – IP Enabled Regional Network

As a result, other devices need to be added to the Regional Network to provide better aggregation of subscriber traffic. There are several options for doing this, most of which involve IP enabling the Regional Network as shown in Figure 4. Subscribers that use native IP, which is a routable protocol, can be aggregated at the IP level into a Virtual LAN (VLAN) or Virtual Private Network (VPN) for handoff to their associated Service Provider. Those subscribers that use variations of the Point-to-Point Protocol (PPP), such as PPPoA (PPP over ATM) and PPPoE (PPP over Ethernet), can be aggregated at either the PPP or the IP layer.

If the aggregation is done at the PPP layer, then these PPP sessions will need to be forwarded over a routable protocol such as Layer 2 Tunneling Protocol (L2TP). When the new subscriber aggregation element is functioning in this mode, it is referred to as an L2TP Access Concentrator or LAC. The other option for PPP based subscriber is to also terminate the PPP session and assign IP addresses to the subscribers. This traffic would then be collected into a VLAN or VPN as with native IP traffic. When performing PPP Termination and Aggregation (PTA), the box is typically called a Broadband Remote Access Server or BRAS.

As more and more DSL aggregation is performed at the IP layer rather than the ATM layer, additional transport options may be added. In addition to ATM, Ethernet and Packet over SONET are also options for IP transport. There are various metropolitan Ethernet solutions available in speeds of 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), or 1 Gbps (Gigabit Ethernet or GigE).

These new network elements also need to be able to function as the first tier ATM aggregation device, where the Access Node is now directly connected. As such, these devices will also need to handle ATM level aggregation and switching and need to function as an adjunct to the existing ATM network. Since they are IP aware, they can also serve as the Label Edge Router (LER) that is required if the Core Network is to become Multi Protocol Label Switching (MPLS) aware. This would be shown in Figure 4 by collapsing the BRAS and ATM switch into a single multi-protocol device.

4.2 Logical Elements and Interfaces

4.2.1 Application Service Provider Network

4.2.1.1 Description

The Application Service Provider (ASP) is defined as a Service Provider that uses a common infrastructure provided by the Regional/Access Network and an IP address assigned and managed by the Regional Network Provider. This is a new type of DSL service. The Regional Network Provider owns and procures addresses that they, in turn, allocate to the subscribers. ASPs then use this common infrastructure in order to provide application or network services to those subscribers. For example, an ASP may offer gaming, Video on

Demand, or even filtered Internet access, or access to VPNs via IPsec or some other IP-tunneling method. The ASP service may be subscriber-specific, or communal when an address is shared using Network Address Port Translation (NAPT) throughout a Customer Premises Network (CPN). It is envisioned that the ASP environment will have user-level rather than network-access-level identification, and that a common Lightweight Directory Access Protocol (LDAP) directory will assist in providing user identification and preferences. Logical elements used by ASPs typically include routers, application servers, and directory servers. The relationship between the ASP Network, the A10-ASP interface, and the Regional Network is shown in Figure 2. There is one and only one ASP network per Regional/Access Network.

4.2.1.2 Capabilities

The capabilities of the ASP include but are not limited to the following:

- Authenticating users at the CPN
- Assignment of user profile or preference data
- Assignment of QoS to service traffic
- Customer service and troubleshooting of network access and application-specific problems
- Ability to determine traffic usage for accounting purposes and billing

4.2.2 A10-ASP Interface

4.2.2.1 Functionality

As shown in Figure 5, the A10-ASP interface defines the interworking between the ASP Network and the Regional/Access Network. This is not a traditional interface. However, in order to provide more technical and business options to would-be broadband content and application providers this document defines a way for a Service Provider to attach a server, servers, or entire network to a common infrastructure directly accessible by DSL subscribers. The A10-ASP interface is intended to promote content on demand, IP telephony, gaming, and other Quality of Service (QoS) or Bandwidth on Demand (BoD) applications without the need to deploy or manage an IP infrastructure. This also conserves IP addresses, as a single address can be used to gain access to all the services and providers that opt to share this infrastructure.

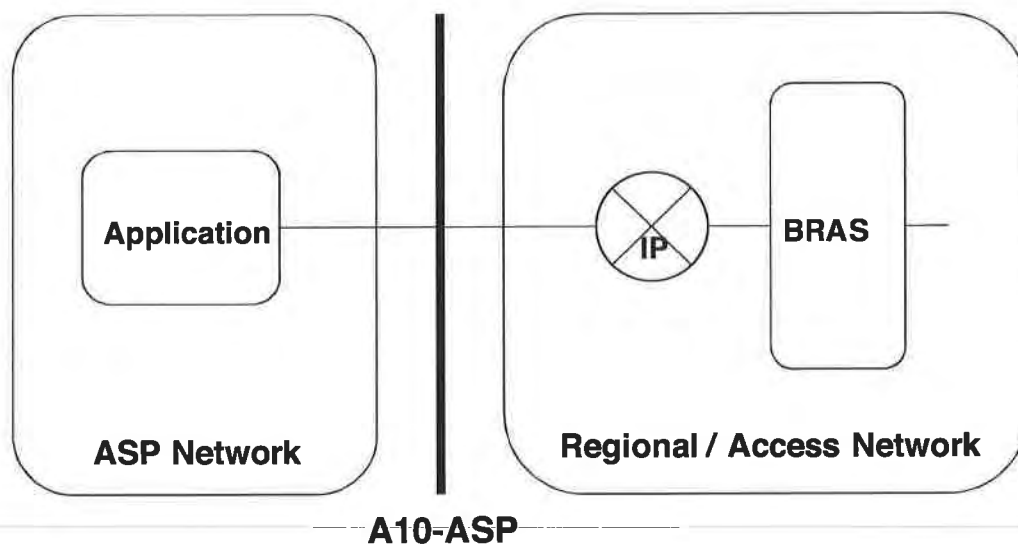


Figure 5 – A10-ASP Interface

4.2.2.2 Communication Protocols

This interface MUST_[1] support IP networking connectivity to the DSL subscribers. Several QoS and BoD use cases exist:

1. Best effort IP networking is used with no additional QoS or information required.
2. Differentiated Services (Diffserv) QoS is provided in order to establish a higher class of service – oriented toward higher throughput, packet precedence, or lower latency.
3. QoS and Bandwidth limitations can be enforced by the Regional/AccessNetwork based on provisioned relationships between the ASP and all users or potentially specific users.

The communications protocol stack is shown in the following Figure 6.

A10-ASP

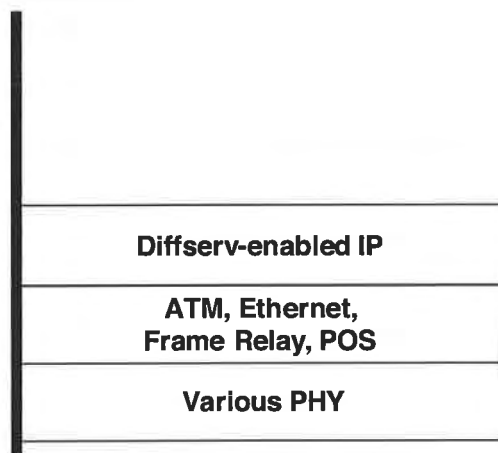


Figure 6 – ASP Protocol Stack with QoS

The ASP obtains an IP connection over a typical data link layer as described earlier. More likely is that an ASP actually obtains a 10 Base-T, 100 Base-T, or GigE connection to the Regional/Access Network within a co-location or hosting facility. The Regional/Access Network provider statically assigns addresses to the A10 ASP interfaces, and MAY_[2] provide address blocks to the ASP.

Network Layer

The network layer interface MUST_[3] support IP version 4 in accordance with IETF RFCs 791 and 2474.

The network layer MAY_[4] support IP version 6 in accordance with IETF RFC 2460.

The network layer interface SHOULD_[5] support IP multicast.

The network layer interface MUST_[6] support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140 when that type of QoS is offered. In other words, IP QoS will use Diffserv instead of using TOS bits or other potential indicators and definitions.

Data Link Layer

The data link layer SHOULD_[7] support Ethernet in hosting or co-location sites.

The data link layer MAY_[8] support ATM, Frame Relay, and/or POS.

The data link layer MAY_[9] support bonding of multiple physical interfaces.

Physical Layer

The physical layer interface MUST_[10] support at least one of the following – as appropriate:

- Ethernet PHY for 10 Mbps, 100 Mbps, 1 Gbps
- DS1, DS3, E1, E3
- OC3c, OC12c, OC48c, STM1c, STM4c, STM16c

4.2.3 Network Service Provider Network

4.2.3.1 Description

The Network Service Provider (NSP) is defined as a Service Provider that provides addressing and connectivity to an Internet Protocol (IP) network. This is the typical application of DSL service today. The NSP owns and procures addresses that they, in turn, allocate individually or in blocks to their subscribers. The subscribers are typically located in Customer Premises Networks (CPNs). The NSP service may be subscriber-specific, or communal when an address is shared using NAPT throughout a CPN. This relationship among the NSP, A10-NSP interface, and Regional/Access Network is shown in Figure 2. NSPs typically provide access to the Internet, but may provide access to a walled garden, VPN, or some other closed group or controlled access services. L2TP and IP VPNs are typical A10-NSP interface arrangements.

The capabilities of the NSP include but are not limited to the following:

- Authenticating network access between the CPN and the NSP network
- Assignment of network addresses and IP filters
- Assignment of traffic engineering parameters
- Customer service and troubleshooting of network access problems

4.2.4 A10-NSP interface

4.2.4.1 Functionality

As shown in Figure 7 and Figure 9, the A10-NSP interface defines the interworking between the NSP and the Regional/Access Network provider. This document offers the following Layer 2 and Layer 3 options for this interconnection.

4.2.4.2 Communication Protocols: L2TP Connection

This interface MUST_[11] support the Layer 2 PPP connection service supported by L2TP. Using Figure 8 as a reference, subscribers MUST_[12] be placed into L2TP tunnels in one of the following methods:

1. L2TP tunnels MAY_[13] be established or provisioned statically between LNS and the LAC or through an intervening Layer 2 Tunnel Switch (L2TS).
2. L2TP tunnels MAY_[14] be established dynamically using RADIUS in order to determine which users to add to various L2TP tunnels, including potentially new ones. As before, these may be directly between LAC and LNS or via L2TS.

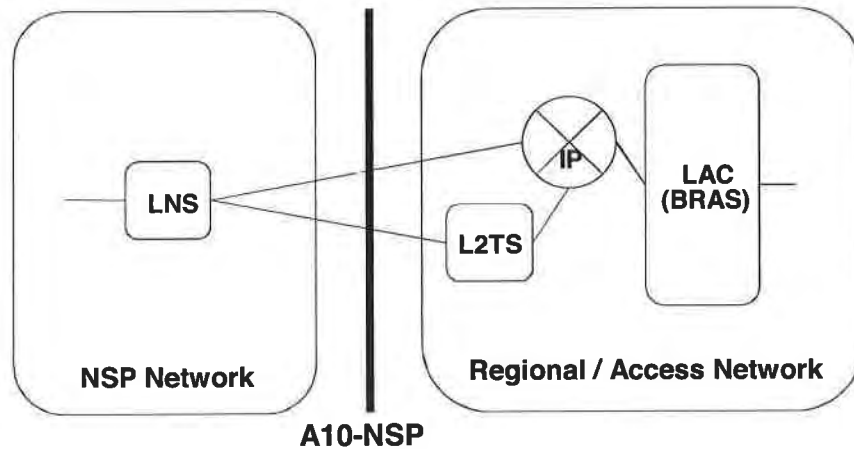


Figure 7 – A10-NSP Interface Supporting L2TP Connection

One or more concurrent sessions can be established to NSPs from any given CPN, and the destinations are chosen by the fully qualified domain name (FQDN) of the accessing subscriber.

Business models that require limiting subscriber access to a single NSP SHOULD_[15] be supported through administrative limits on the FQDN routing established by the Regional/Access Network provider on behalf of one or more NSPs. Subscribers SHOULD_[16] be able to establish multiple access sessions to the same or to different NSPs.

The RADIUS response MAY_[17] be used to determine the bandwidth profile for its access session. Note that RADIUS will require enhancement to do this in a standard way.

The communications protocol stack is shown in the Figure 8.

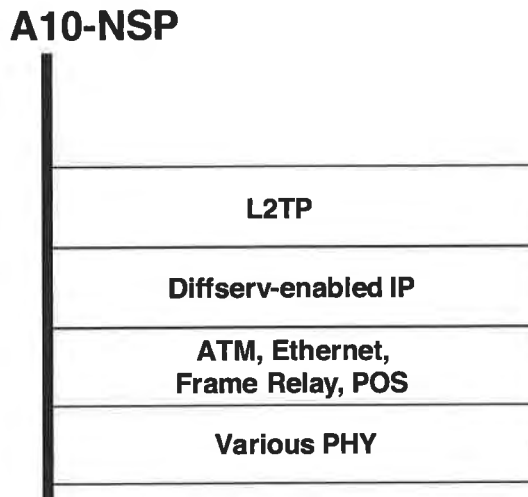


Figure 8 – L2TP Protocol Stack

While L2TP over IP is always used, as opposed to L2TP delivered directly over ATM or Frame Relay, various IP transport options can be provided by the Regional/Access Network provider or selected by the NSP according to availability, regulation, and economics. Also, while the entire L2TP tunnel can be provided with a traffic engineering specification, the constituent flows within an L2TP tunnel will not receive differentiated service. In other words all the flows within an L2TP tunnel will receive the same aggregate QoS treatment.

Network Layer

The network layer interface MUST_[18] support IP version 4 in accordance with IETF RFCs 791 and 2474.

The network layer MAY_[19] support IP version 6 in accordance with IETF RFC 2460.

The network layer MUST_[20] make use of L2TP over IP in accordance with IETF RFC 2661.

Data Link Layer

The data link layer SHOULD_[21] support ATM.

The data link layer MAY_[22] support Ethernet, Frame Relay, and/or POS.

The data link layer MAY_[23] support bonding of multiple physical interfaces.

Physical Layer

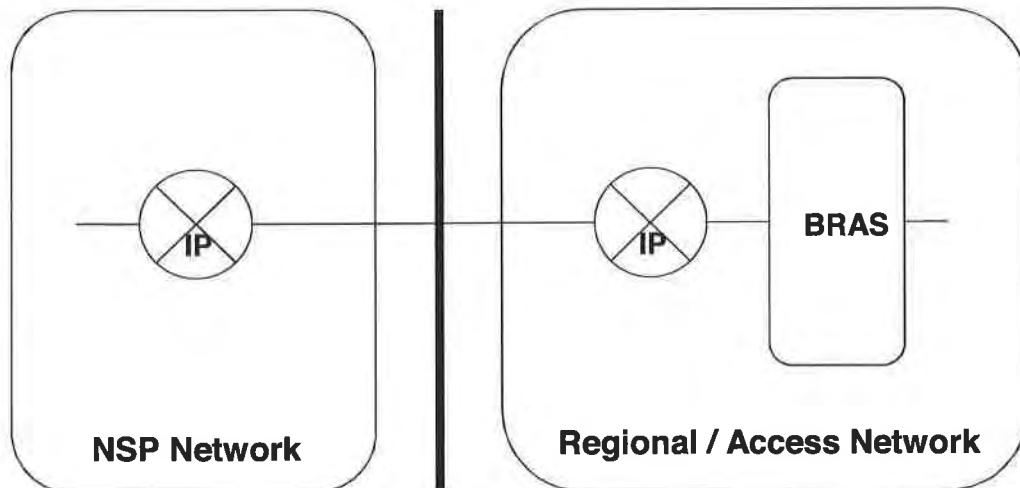
The physical layer interface MUST_[24] support at least one of the following – as appropriate:

- Ethernet PHY for 10 Mbps, 100 Mbps, 1 Gbps
- DS1, DS3, E1, E3
- OC3c, OC12c, OC48c, STM1c, STM4c, STM16c

4.2.4.3 Communication Protocols: IP Routed Connection

This interface MUST_[25] support the Layer 3 IP routed connection. Using Figure 9 as a reference, subscribers MUST_[26] be placed into IP routed networks in one of the following methods:

1. IP address pools MAY_[27] be established or provisioned statically.
2. IP addresses MAY_[28] be provided in pools that are distributed dynamically by the Regional/Access Network provider.
3. Subscribers IP addresses MAY_[29] be distributed from the NSP to the BRAS dynamically using RADIUS.
4. IP addresses MAY_[30] be assigned from named pools in cases where the NSP opts to allocate addresses out of two or more pools based on subscriber-specific information.



A10-NSP

Figure 9 – A10-NSP Interface Supporting IP Routed Connection

In every case, RADIUS MUST_[31] be used between the BRAS (or a potential RADIUS proxy) and an NSP-designated AAA system or systems to authenticate subscriber access to the routed network.

In most cases, the IP routed network will be comprised of many IP-VPNs that support sharing of the Regional/Access Network at the IP layer.

Multiple services may be offered across the 'U' interface. Access to a particular IP service will be established as with L2TP using the Network Access Identifier (NAI a.k.a. FQDN) provided by the accessing subscriber. Subscribers MUST_[32] be able to establish multiple access sessions to the same or to different NSPs. Business models that require restricting simultaneous access to particular combinations of IP service MUST_[33] be supported through administrative policies established in the regional/access network on behalf of the NSPs/ASPs.

If an NSP connects to the Regional/Access Network in several places, the A10-NSP interface SHOULD_[34] support BGP4 as per IETF RFC 1745.

Several QoS and BoD use cases exist:

1. Best effort IP networking is used with no additional QoS or information required.
2. Diffserv QoS MAY_[35] be supported and MAY_[36] be used in order to establish a higher class of service – oriented either toward higher throughput, or lower latency.
3. The Regional/AccessNetwork can enforce QoS and Bandwidth limitations based on provisioned relationships between the NSP and all users or potentially specific users.

The communications protocol stack is shown in Figure 10.

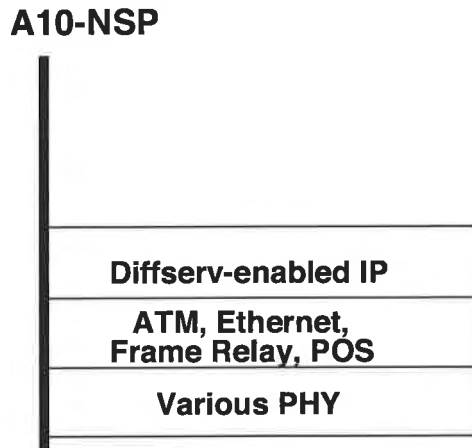


Figure 10 – Routed IP Protocol Stack with QoS

IP MUST_[37] always be used; however, various IP transport options can be provided by the Regional/Access Network provider or selected by the NSP according to availability, regulation and economics. As described earlier, RADIUS MUST_[38] always be used to authenticate users, SHOULD_[39] be used to set NSP-desired filters, and MAY_[40] be used to assign addresses.

Network Layer

The network layer interface MUST_[41] support IP version 4 in accordance with IETF RFCs 791 and 2474.

The network layer interface MUST_[42] support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140 when this type of QoS is offered.

The network layer interface SHOULD_[43] support IP multicast.

The network layer interface MUST_[44] support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140 when this type of QoS is offered.

The network layer MAY_[45] support IP version 6 in accordance with IETF RFC 2460.

Data Link Layer

The data link layer SHOULD_[46] support ATM

The data link layer MAY_[47] support Ethernet, Frame Relay, and/or POS.

The data link layer MAY_[48] support bonding of multiple physical interfaces.

Physical Layer

The physical layer interface MUST_[49] support at least one of the following – as appropriate:

- Ethernet PHY for 10 Mbps, 100 Mbps, 1 Gbps
- DS1, DS3, E1, E3
- OC3c, OC12c, OC48c, STM1c, STM4c, STM16c

4.2.5 Regional/Access Network

The Regional/Access Network consists of the Regional Network, Broadband Remote Access Server, and the Access Network as shown in Figure 11. Its primary function is to provide end-to-end transport between the customer premises and the NSP or ASP. The Regional/Access Network may also provide higher layer functions such as QoS and content distribution. QoS will be provided by tightly coupling traffic-engineering capabilities of the Regional Network with the capabilities of the BRAS. Depending on the type and frequency of use, certain content storage may be pushed further out in the Regional/Access Network than others. As a result, functionality to support content distribution could be located at different points within the Regional/Access Network, but will not be located between the BRAS and the subscriber.

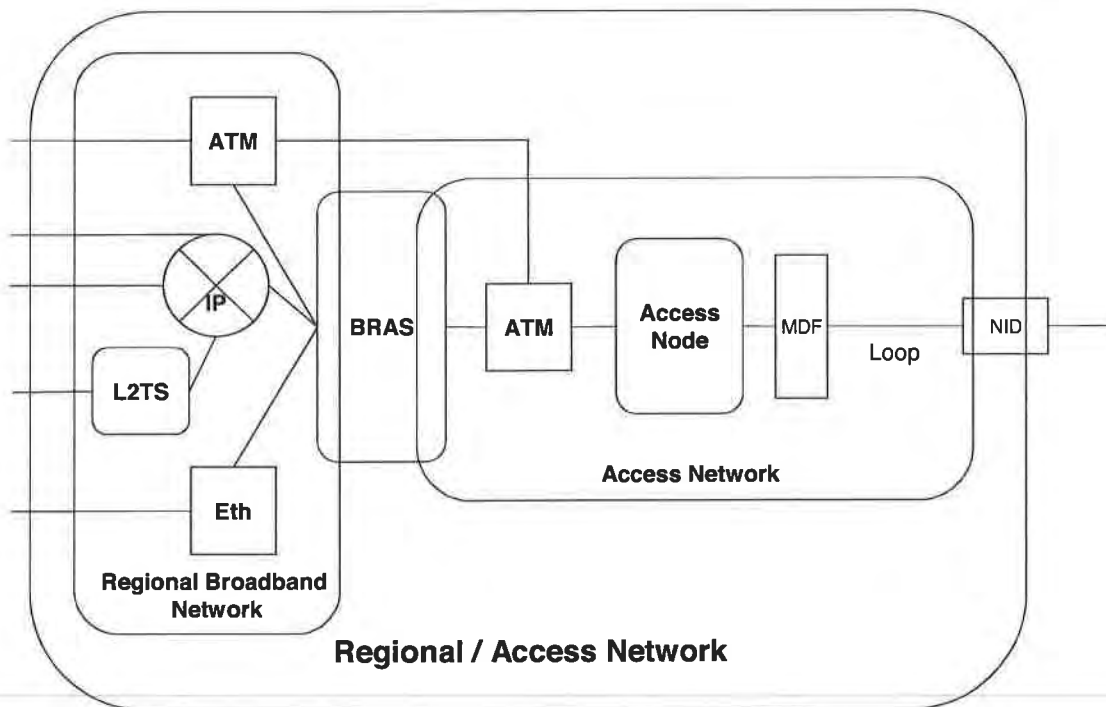


Figure 11 – Components of the Regional/Access Network

4.2.5.1 Regional Network

The Regional Network connects one or more BRAS and associated Access Network to NSPs and ASPs. It supports aggregation of traffic from multiple Access Networks and hands off larger geographic locations to NSPs and ASPs – relieving a potential requirement for them to build infrastructure to attach more directly to the various Access Networks. This arrangement is shown in Figure 12, which pictures an NSP and an ASP attached to a Regional Network in order to gain access to 3 Access networks. This architecture assumes that the network providers of the Regional and Access Networks work extremely closely in order to provide an end-to-end QoS solution. A good assumption might be that the 2 networks are operated and managed by a single service providing entity and offered as a combined, Regional/Access Network.

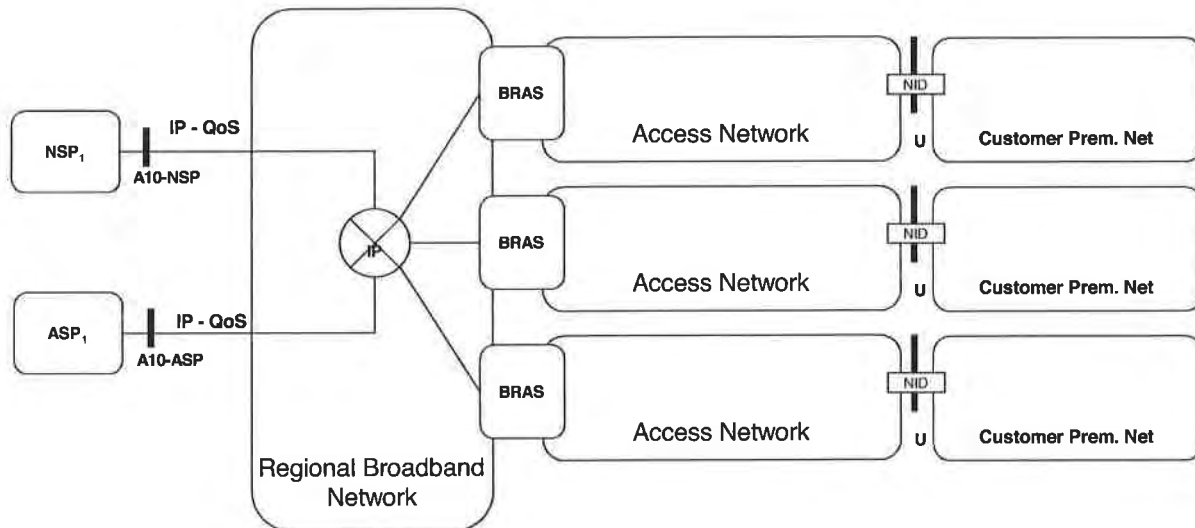


Figure 12 – Aggregation function of Regional Network

The Regional Network may transport traffic using ATM, Ethernet, IP or MPLS. Within these networking technologies, the Regional Network MUST_[50] provide scalable traffic engineering capabilities and preserve IP QoS.

4.2.5.2 Broadband Remote Access Server

The BRAS performs multiple functions in the network. Its most basic function is to provide aggregation capabilities between the Regional/Access Network and the NSP/ASP. For the aggregation Internet traffic, the BRAS serves as a L2TP Access Concentrator (LAC) tunneling multiple subscriber PPP sessions directly to an NSP or switched through a L2TS. It also performs aggregation for terminated PPP sessions or routed IP session by placing them into IP VPNs or 802.1Q VLANs. The BRAS also supports ATM termination and aggregation functions.

Beyond aggregation, the BRAS is also the injection point for providing policy management and IP QoS in the Regional and Access Networks. The BRAS is fundamental to supporting the concept of many-to-many access sessions.

Policy information can be applied to terminated and non-terminated sessions. For example, a bandwidth policy may be applied to a subscriber whose PPP session is aggregated into an L2TP tunnel and is not terminated by the BRAS. However, sessions that terminate on (or are routed through) the BRAS can receive per flow treatment because the BRAS has IP level awareness of the session. In this model, not only can the aggregate bandwidth for a customer be controlled but also the bandwidth and treatment of traffic on a per application basis.

The delivery of content has shifted from content that was more download intensive with lower bandwidth and best effort quality to one that is more real-time in nature, requiring higher bandwidth with higher quality. Some of the higher bandwidth applications include Video on Demand (VoD) for movies, multicast ("Broadcast" TV), and MPEG unicast video. Given the BRAS's proximity to the edge of the network and its ability to support IP

services, the BRAS SHOULD_[51] also provide support for content distribution and efficient use of multicast services.

Some high level functional requirements are for the BRAS are listed below. This list is not comprehensive and additional requirements for QoS are listed in Section 5. Additionally, BRAS requirements from both this architecture as well as other architectures are expected to become a separate DSL Forum topic.

- The BRAS MUST_[52] be able to aggregate PPP sessions into L2TP tunnels (LAC function).
- The BRAS MUST_[53] be able to terminate PPP sessions and assign routing attributes based on subscriber profile (LNS function).
- The BRAS MUST_[54] support authentication using RADIUS.
- The BRAS MUST_[55] support IP over bridged Ethernet (IETF RFC 2684).
- The BRAS MUST_[56] support address allocation using Dynamic Host Configuration Protocol (DHCP).
- The BRAS MUST_[57] support multiple VCs per subscriber.
- The BRAS SHOULD_[58] support ATM VC/VP cross-connection functions independent of AAL type.
- The BRAS MUST_[59] support termination and aggregation of ATM VCs.
- The BRAS SHOULD_[60] support the following ATM classes of service: UBR, UBR+, CBR, VBR-nrt, VBR-rt .
- The BRAS MUST_[61] allocate downstream bandwidth based on policy configuration across ATM, PPP, Ethernet, and IP technologies.
- The BRAS MUST_[62] mark IP QoS fields for upstream and downstream traffic based on policy configuration.
- The BRAS MUST_[63] support policing of upstream per-subscriber traffic based on policy configuration.
- The BRAS MUST_[64] support queuing and prioritization based on diffserv marking and/or flow classification.
- The BRAS MUST_[65] support traffic engineering for networking technologies including ATM, MPLS, and Ethernet.
- The BRAS MUST_[66] support a Diffserv-aware hierarchical scheduler that allows it to manage the network so that any potential congestion in the Access Network between the BRAS and the RGs is avoided. The hierarchical scheduler in the BRAS MUST_[67] be able to model the congestion points in at least two subsequent ATM hops (corresponding to the daisy chaining of two ATM switching/multiplexing points in the Access Node); if the BRAS does not include the ATM switching function, then the hierarchical scheduler in the BRAS MUST_[68] be able to model the congestion point in yet an additional ATM hop. This scheduler is described in further detail in section 5 and shown by example in Appendix B.
- The BRAS MUST_[69] shape the individual subscriber's aggregate downstream traffic to the subscribed rate which will be some value equal to or lower than the DSL sync rate.
- The BRAS MUST_[70] support RED and WRED policing of upstream traffic using the same topology information that exists for the hierarchical scheduler.
- When operating in an IP-routed mode, the BRAS MAY_[71] provide multicast support
- The BRAS SHOULD_[72] support Ethernet LAN interfaces for the local attachment of content distribution servers.
- When operating in an IP-routed mode the BRAS MAY_[73] provide multicast access control and collect multicast usage information.

4.2.5.3 Access Network

Description

The Access Network refers to the network between the NID and the BRAS. The protocols between these devices are well defined and this recommendation does not attempt to alter them.

4.2.5.4 Access Node

Description

The Access Node contains the XTU-C, which terminates the DSL signal. Physically, the XTU-C can be deployed in the central office in a DSLAM, or remotely in a remote DSLAM (RT-DSLAM), Next Generation Digital Loop Carrier (NG-DLC), or a Remote Access Multiplexer (RAM). A DSLAM hub can be used in a central office to aggregate traffic from multiple remote physical devices, and is considered logically to be a part of the Access Node.

The Access Node provides aggregation capabilities between the Access Network and the Regional Network. It is the first point in the network where traffic on multiple DSL lines will be aggregated onto a single network. Traditionally the Access Node has been primarily an ATM concentrator, mapping PVCs from the DSL modem to PVCs in the ATM core. It has also shaped and policed traffic to the service access rates.

The role of the Access Node will change slightly in this architecture. While it will remain in the aggregation role, the current responsibility of policing DSL modem-to-BRAS PVCs to the subscribed line rate will be moved from the Access Node to the BRAS in order to establish additional bandwidth on the DSL line for additional services. The Access Node will set line rate for each PVC at the synch rate (or slightly less) of the DSL Modems. This will make the maximum amount of subscriber bandwidth available for services. The BRAS will retain the ability to police individual sessions/flows as required to their existing rates and will also perform the dynamic changes when bandwidth-on-demand services are applied. In order to do this the BRAS MUST_[74] be provisioned so that it does not allow traffic to flow faster than the DSL sync rate. The BRAS MAY_[75] be provisioned with the actual DSL sync rate to accomplish this.

Various physical Access Node configurations are shown in Figure 13, with brief names for the configurations listed in Table 1.

In order to allow IP QoS support over an existing non-IP-aware layer 2 network without using multiple layer 2 QoS classes, a mechanism based on hierarchical scheduling is used. This mechanism, which is further described in section 5, preserves IP QoS over the ATM network between the BRAS and the RGs by carefully controlling downstream traffic in the BRAS, so that significant queuing and congestion does not occur further down the ATM network. This is achieved by using a hierarchy of scheduling steps in the BRAS that will account for downstream trunk bandwidths and DSL synch rates. As the depth of non-IP aware nodes between the BRAS and RG increases, the complexity of implementing hierarchical scheduling grows as well. In order to minimize this complexity, the daisy chaining MUST NOT_[76] exceed a depth of more than two ATM switching / multiplexing points including the Access Node and subtending Access Nodes. Additionally, if the BRAS does not incorporate an ATM pass-through or switching functionality, an additional layer of hierarchical scheduling MUST_[77] be used to manage the trunk to the ATM switch.

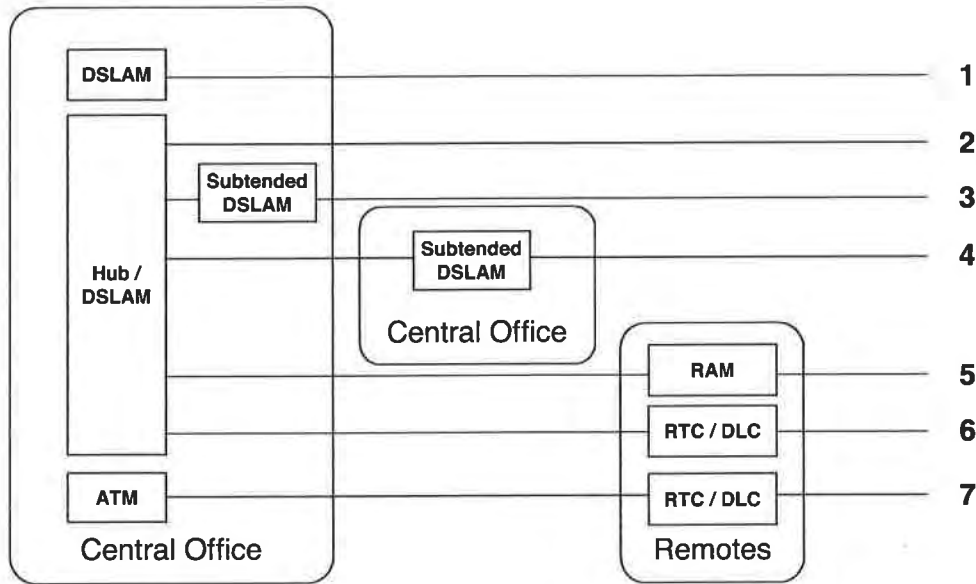


Figure 13 – Access Node Architecture Variations

Table 1 – Access Node Architecture Variation Descriptions

Reference #	Description
1	Access Node
2	Hub Access Node
3	Collocated Subtended Access Node
4	Remotely Located Subtended Access Node
5	Subtended Remote Access Node
6	Subtended DLC Located Access Node
7	Aggregated DLC Located Access Node

4.2.6 U Interface

4.2.6.1 Functionality

The U interface is defined as the interface between the Access Network and the CPN. This interface refers to the area between the CPN where the DSL modem is located and the Access Network where the Access Node is located – usually in the NID. The U interface includes the capabilities and protocols that cross between the Access Network and the CPN.

4.2.6.2 Communication Protocols

As shown in Figure 14 the U interface defines the interworking between the CPN and the Regional/Access Network. This interface MUST_[78] support the bi-directional delivery of data for all the new product and service definitions as well as for existing (legacy) products and services.

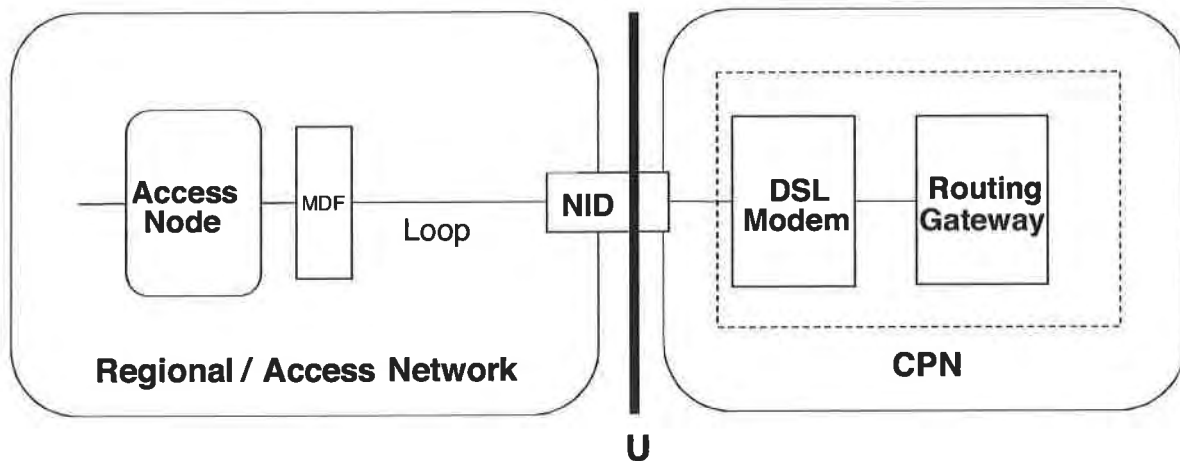


Figure 14 – U Interface

Although the first Network Element connection in the network is at the Access Node, the U interface MUST_[79] support the transparent flow of protocols from the DSL Modem to the BRAS.

- The U interface MUST_[80] support at least one ATM AAL5 PVC per CPN using PPPoE and/or IP over Ethernet (IETF RFC 2684 configured using DHCP). Although the target architecture to support QoS enabled IP services seeks to utilize a single ATM AAL5 PVC per CPN, it is recognized that certain required network element features identified in this document have yet to be developed. In particular, dynamic packet fragmentation/MTU sizing in the CPE (needed to control jitter and delay for short packet/high priority applications) may trail the availability of other required network element features. In order to meet the demands of service descriptions previously identified in an acceptable timeframe, a second ATM PVC may be provisioned to provide a means to separate those application flows having tight jitter and latency requirements. This second PVC will require that DSL modems support multiple PVCs. In the event that 2 PVCs are provisioned, it is desired that they be treated as a PVC bundle as this feature is made available. Additionally the PVC bundle standards need to be enhanced to support bridged Multi-service traffic.
- The U interface MUST_[81] support Diffserv Code Points (DSCP) per IETF RFCs 2474 and 3260, enabling application-layer QoS access.
- The U interface MUST_[82] support the ability to dynamically push IP routes back to the customer PC or Routing Gateway. Thus, RIPv2 will be used to provide routes to the RG. The RG is not expected to provide routes to the WAN.
- The BRAS SHOULD_[83] support a mechanism to push routing information to the RG at the start of a PPP session.

The communications protocol stack is shown in the following figure.

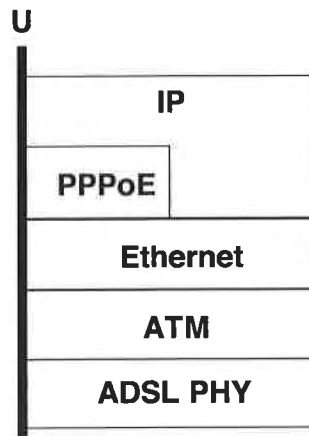


Figure 15 – U Interface Protocol Stack

Network Layer

The network layer interface MUST_[84] support IP version 4 in accordance with IETF RFCs 791 and 2474.

The network layer MAY_[85] support IP version 6 in accordance with IETF RFC 2460.

The network layer interface MAY_[86] support IP precedence based on Diffserv Code Point (DSCP) markings, in accordance with IETF RFC 3140.

The network layer interface MUST_[87] support PPPoE per IETF RFC 2516.

Data Link Layer

The data link layer MUST_[88] support Ethernet encapsulation in accordance with IETF RFC 2684.

The data link layer MUST_[89] support ATM in accordance with ATM Forum standards.

Physical Layer

The physical layer interface MUST_[90] support G.dmt, and its related standards.

4.2.7 Customer Premises Network

The Customer Premises Network (CPN) is defined at its highest level as the location where the ATU-R is located and terminates the physical DSL signal, and where the subscriber's computers and other devices are interconnected. The initial DSL deployments focused on single user architectures where the CPN constituted a single PC connected directly to a DSL modem. This paradigm of service will continue to be supported and improved, but must be extended to support advanced features that go beyond the single user model. To support enhanced features (multi-user, gaming, VoIP, video, etc), the CPN must evolve to support the networking and management of devices and services within the home or business location.

From a network perspective, the CPN is the ultimate target of the services provided by the Service Provider (NSP or ASP). The CPN includes the networking environment and protocols that are resident in the premises. A CPN may imply coexistence of different link and physical layer technologies such as radio, power line transmission and Ethernet, but is assumed to have access to outside networks (via DSL). The terms devices and appliances refer to the collection of end terminals that can reside on the CPN, either temporarily (laptops, palm pilots, foreign devices etc.) or permanently, such as desktops, security, and climate control systems. Devices may or may not be individually addressable and reachable from other devices, inside or outside the CPN. Some devices may communicate with proxies that then can relay or translate state or configuration information for these end devices.

4.2.7.1 DSL Modem

Description

The DSL Modem terminates both DSL and ATM. It may or may not be integrated with additional Routing Gateway (RG) functionality. If it is not integrated, it will be used in a mode that is referred to as a simple bridge modem.

Capabilities

The capabilities of the DSL Modem in support of this architecture MUST^[91] include but are not limited to the following:

- 2 ATM AAL5 PVCs - in order to be able to support the U interface service option of using 2 PVCs as described in 4.2.6.2. Note that in practice, DSL modems will likely have additional service drivers that would require them to support additional PVCs.
- UBR, UBR+ and VBR-rt ATM classes of service
- Per-VC queuing, separate priority queues for ATM classes of service

4.2.7.2 Routing Gateway

Description

CPN architectures typically leverage a Routing Gateway (RG) device that provides functionality beyond that of a basic DSL modem. The RG may or may not be integrated with the DSL modem function. In the integrated scenario, the device terminates the DSL signal from the network and provides an interface to other equipment located within customer premises. In the non-integrated case, the RG is physically separate from the DSL modem and adds functionality to the CPN independent of the DSL modem.

The principal tasks of the RG are to shape upstream traffic to the policed rate at the BRAS, to provide appropriate queuing and precedence for QoS traffic, and to allow a home network to share a single public address for network access. The data required for these duties may be pre-provisioned, user-provisioned or may be provisioned using an automatic configuration protocol. For an example of this third case, the RG may query a configuration server in the Regional / Access Network in order to learn the upstream policing rates for its access connections – and in the case of a non-integrated RG it may also learn the upstream sync rate of the detached ATU-R.

Since the integrated RG has knowledge of the CPN and its access to external networks, it enables tighter control of QoS for real time applications than may be possible in a non-integrated architecture. Both integrated and non-integrated RG are supported in this specification.

Capabilities

To support this QoS-enabled architecture, the capabilities of the RG MUST include but are not limited to the following:

- IP routing between the CPN and the Access Network ^[92]
- Multi-user, multi-destination support: Multiple simultaneous PPPoE sessions (started from the RG or from devices inside the CPN) in conjunction with non-PPP encapsulated IP (bridged) sessions per IETF RFC 2684. ^[93]
- Network Address Port Translation (NAPT) ^[94]
- Local DHCP ^[95]
- Support for major applications and protocols in the presence of NAPT and firewall (e.g., SIP, H.323, IPsec) ^[96]
- Dynamic MTU negotiation ^[97]
- Packet segmentation based on traffic/queue type ^[98]

- PPPoE pass through^[99]
- Multiple queues, with the appropriate scheduling mechanism. ^[100]
- IP QoS
 - Classification, scheduling and shaping of IP flows^[101]
 - Diffserv^[102]
 - Management interface^[103]
 - Support for real time services (Voice, Video) ^[104]
 - Re-marking capabilities^[105]
- If 2 VCs are provisioned, support the mapping between Diffserv Code Point (DSCP) and a specific PVC (Using a PVC bundle is the desired way to meet this requirement) ^[106]

4.2.7.3 Networking Technologies

Description

The CPN will support the transparent transmission of IP packets. It is expected that the CPN will be a hybrid of technologies that may include Ethernet, phone line networking, power line networking, wireless networking, and others.

4.2.7.4 LAN Devices

Description

Devices inside the CPN that are served by the DSL Modem and RG, and connected by the various Networking Technologies are referred to as LAN Devices. These may include, but are not limited to, PCs, laptops, networked set-top boxes, and Internet Appliances.

4.2.8 T Interface

4.2.8.1 Functionality

As shown in Figure 16, the T interface defines the interworking between the DSL modem/RG and the LAN Devices. This interface MUST^[107] support the bi-directional delivery of IP packets between the RG and other CPE as well as the ability to assign addresses to other CPE using DHCP. The other major functional requirement placed on the T interface includes identifying and supporting "QoS flows" as defined in Section 5. The primary goal of this interface is to facilitate seamless transmission of IP packets in both a best effort approach as well as maintaining predefined QoS behavior.

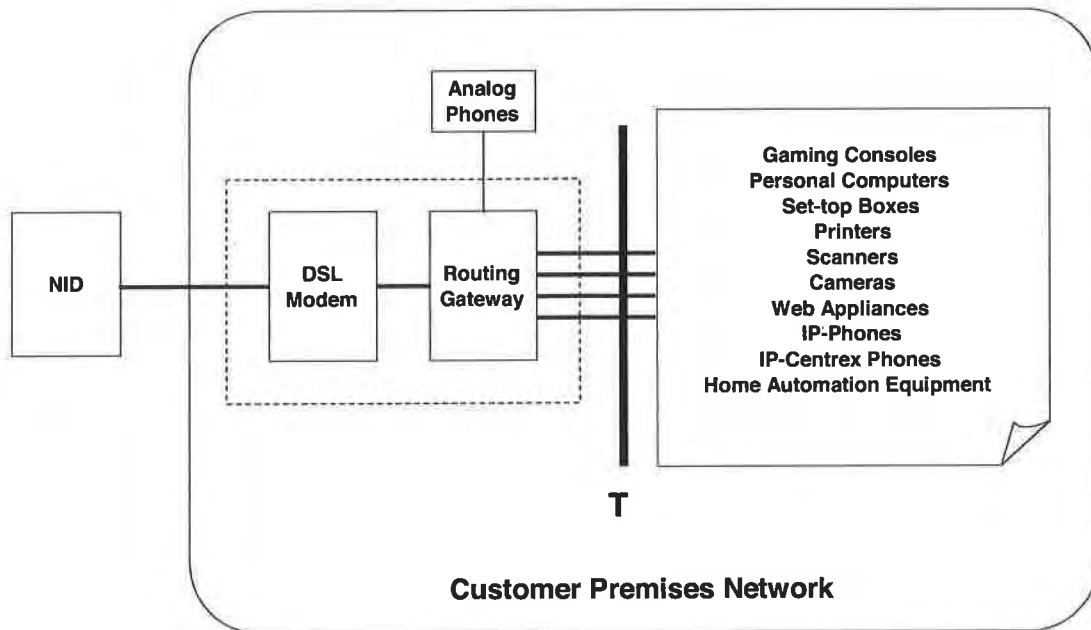


Figure 16 – T Interface

4.2.8.2 Communication Protocols

Network Layer

The network layer interface MUST_[108] support IP version 4 in accordance with IETF RFCs 791 and 2474.

The network layer MAY_[109] support IP version 6 in accordance with IETF RFC 2460.

The network layer interface MUST_[110] support differentiated service (Diffserv) code points in accordance with IETF RFC 3140.

Data Link Layer

The data link layer MUST_[111] support Ethernet in accordance with IEEE 802.2/802.3 (Ethernet) and as shown in Figure 17.

The data link layer SHOULD_[112] support Ethernet virtual LANs (IEEE 802.1Q).

The data link layer SHOULD_[113] support IEEE 802.1D/Q.

The data link layer MUST_[114] support PPP over Ethernet in accordance with IETF RFC 2516 and as shown in Figure 18

Logical Link Controller (LLC) Sublayer

The logical link controller sublayer subinterface MUST_[115] support Ethernet in accordance with IEEE 802.2.

Medium Access Control (MAC) Sublayer

The medium access control sublayer subinterface MUST_[116] support Ethernet in accordance with IEEE 802.3.

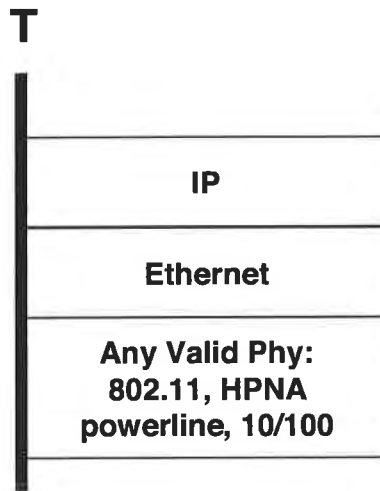


Figure 17 – IP over Ethernet

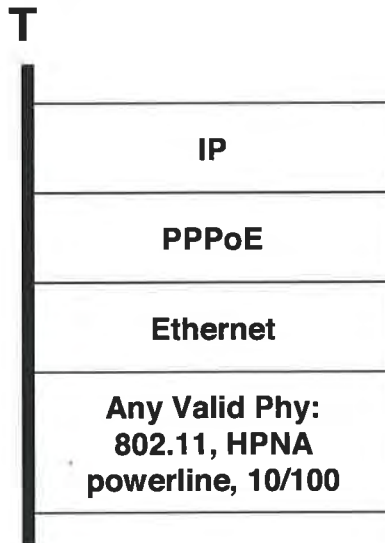


Figure 18 – IP over PPP over Ethernet

5 QUALITY OF SERVICE

5.1 Introduction

DSL architectures and products are predominately engineered for the support of best effort Internet traffic. Many NSPs desire the ability to improve their best effort product by using different levels of over subscription. Additionally, there are other market drivers pushing the Regional/Access Network to support differentiated services that require functionality beyond a best effort grade of service. Such services include telephony, video services, gaming, bandwidth on demand, and corporate VPN access as referenced in section 2.2. In order to support IP services effectively, the network MUST_[117] be IP aware and provide support that scales as the number of DSL subscribers and the number of applications per subscriber increases.

5.1.1 Goals

The goal of this section is to describe the mechanisms for introducing:

- A method for providing different engineered performance to different networks – even for best effort traffic
- Per flow IP QoS into the Regional/Access Network

Both of these goals leverage the existing capital investments yet effectively meet the goals for supporting differentiated non-real time and real-time IP applications.

One goal of the architecture is to enable more flexible bandwidth allocation to customers. It is a goal to allow both the customer and the various Service Providers to participate in defining the bandwidth that will be made available to them via DSL. This bandwidth can be provided at different rates not only at provisioning time or via service orders, but also on demand in near real time using mechanisms like “turbo buttons” at NSP or ASP web interfaces, or by using signaling protocols. It should be noted that this is still best effort bandwidth – there is no guarantee that an application can make use of the maximum bandwidth, in other words there are no throughput guarantees – only that the possible maximum rate might be increased.

Real-time applications have concerns beyond bandwidth, like jitter and latency, which become harder to manage when the DSL line rate slows down. Other applications, while may not be real time, have delivery requirements (no packets dropped) that cannot be assured by bandwidth alone. It is a goal to manage multiple applications over a small number (1 or 2) of ATM PVC(s) between the DSL modem and BRAS and provide the characteristics that both real-time and non-real time applications require.

5.1.2 Assumptions

Existing Regional Networks have a large embedded base of ATM equipment that is not IP aware. This equipment will be leveraged to the extent that it is technically and economically feasible.

5.2 Traffic Engineering of Best Effort Service

Today's DSL access and Regional Networks are typically engineered to an over subscription ratio picked by the various providers. This has served the market well, but may need to be enhanced as service diversity expands and scope broadens. The concept for traffic engineering best effort service is that an NSP might be able to select an over subscription policy, and that the various NSPs can use that as a tool for providing different grades of service, even in an otherwise best effort model. Using this feature, one NSP may opt for highly over-subscribed infrastructure in order to provide an extremely cost-effective service, while a second NSP might choose a much less over subscribed approach in order to provide a better user experience or a premium service.

5.2.1 Theory of Operation

Traffic engineering (TE) makes use of MPLS TE, ATM VP or VC, and L2TP features in order to provide a specific over subscription rate for that NSP.

As shown in Figure 19, traffic flowing between NSP₁ and CPN₁ is shaped to a large asymmetric configuration through the Regional/Access Network. At the same time, traffic flowing between NSP₂ and CPN₂ is shaped to a smaller symmetric configuration. Finally, ATM or Diffserv techniques can be used at the A10-NSP interface in order to divide the total bandwidth at the interface among potentially disparate tunnel types that traverse it.

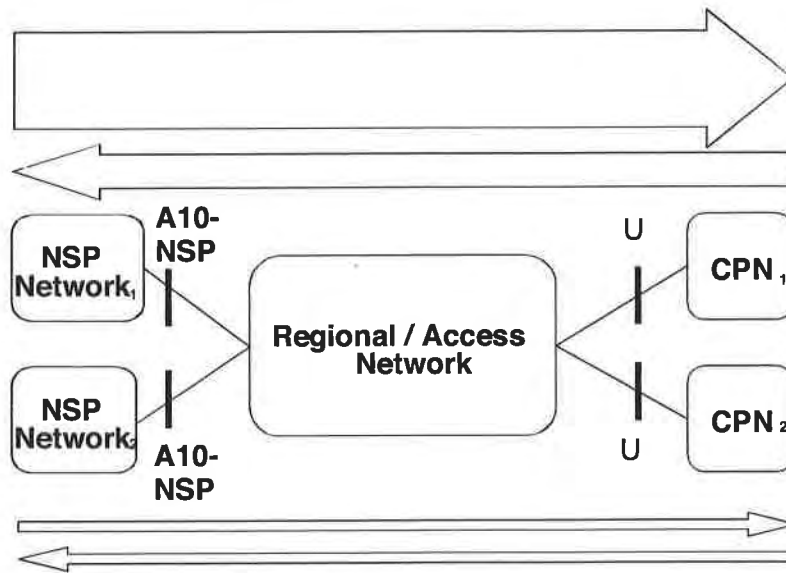


Figure 19 – Best Effort TE

5.3 QoS Architecture - A two-phased approach

While a signaled per flow IP QoS mechanism may ultimately be required for this architecture, the technical and economic feasibility of such a build out can not be justified in the near term. Instead, a 2-phase approach is suggested that leverages incremental IP awareness associated with ATM level traffic engineering. In the first phase, IP aware network elements are added to the network that in conjunction with ATM traffic engineering can manage IP flows through non-IP aware devices. The Diffserv model is leveraged to prioritize and shape traffic through ATM devices. The bandwidth that a subscriber receives will no longer be determined by the DSL synch rate alone. Instead, both the physical and IP layers will be leveraged. Most importantly, phase 1 significantly increases the IP layer functionality of the Regional/Access Network while not requiring massive re-deployment of capital and re-engineering of the network.

Phase 2, however, will require more enhancements to the Regional/Access Network by further increasing the IP capabilities. Policy-based IP QoS is introduced in this phase to allow mass customizability and per-application treatments.

5.3.1 Phase 1 QoS Mechanisms

Phase 1 largely leverages the existing broadband Regional/Access Network as shown in Figure 3. This network is generally IP unaware. In order to efficiently add IP awareness to the network without upgrading the ATM or Access node base, two enhancements are required: Within the network the BRAS is leveraged to provide IP aware handling of traffic and, similarly, at the customer premises new IP aware CPE capabilities are deployed.

One of the goals of this architecture is to provide differentiated services with IP QoS over a non-IP-aware layer 2 network. Since the layer 2 QoS features are not IP aware, they are left unused. Thus traffic from different IP QoS classes is put in the same queues in the layer 2 nodes. Since the layer 2 nodes cannot identify the different IP QoS types within a single queue, congestion MUST_[118] be avoided in all layer 2 network elements at all times in order to retain IP QoS. Furthermore, IP QoS types that offer jitter management will also require that not only congestion is avoided in the L2 queues, but also that significant queuing delays are avoided as well. By avoiding congestion in the layer 2 network, its role is reduced largely to transport, and the switches are modeled like simple multiplexers. This means that the buffering mechanisms in the layer 2 nodes are avoided. Avoiding downstream congestion in the layer 2 network can be achieved by giving the BRAS full awareness of a logical

tree-based network topology. This topology is based on the actual physical and logical topology, but excludes resources that are used by other services (see section 5.3.1.2). The BRAS MUST_[119] be aware of all potential congestion points in this constrained topology, as well as the trunk bandwidths and DSL synch rates. The BRAS MUST_[120] make sure that no more traffic is inserted in the layer 2 network than is allowed according to its knowledge of the logical topology and customer policy constraints. This can be achieved using a hierarchical scheduling mechanism in conjunction with provisioning of services and policies in a way that remains aware of the topological network constraints.

The BRAS MUST_[121] be able to police upstream both for traffic aggregates and for sub-classes of the aggregate using the same topology information that exists for the hierarchical scheduler. The BRAS SHOULD_[122] support random differential drop behavior for upstream traffic aggregates and sub-aggregates based on class. Note that this is required because the RG just has a view of its own DSL line, and doesn't know about the DSL lines that belong to other RGs.

The expectation is that overall admission control for provisioning of bandwidth and the higher tiers of QoS will occur in a policy-based management system that will allow topology, access rates, and business service logic to be applied as part of the provisioning process. The BRAS and RG will enforce the resultant policies.

When a subscriber purchases a differentiated service, this service MUST_[123] flow through the BRAS. To support differentiated services, the BRAS preserves IP QoS downstream through the access node and to the customer premises by means of packet classification, traffic shaping and hierarchical scheduling based on the logical tree-based network topology between the BRAS and the RG.

Once the BRAS is capable of managing the traffic flow through the access node, there is no need for access node to restrict a subscribers connection speed at layer one (ADSL synch rate). Instead, the access node should allow the ATU-R to synch up at its maximum rate. Access sessions will now be shaped and rate limited by the BRAS and can allow for multiple sessions to be individually shaped based on the subscribed service.

The BRAS MUST_[124] support packet classification and scheduling in accordance with DiffServ.

The BRAS MUST_[125] support hierarchical shaping, scheduling, and policing for the control of traffic through the access node and any other intervening devices that do not have IP awareness.

Implementations of hierarchical scheduling MUST_[126] be resource efficient in the sense that any traffic MUST_[127] be capable of using the subscriber bandwidth that has been allocated to that traffic class and that different classes should be able to make use of the unused subscriber bandwidth of other traffic classes.

The effectiveness of using hierarchical scheduling across non-IP aware devices decreases as the number of devices and the amount of non-BRAS controlled traffic increases. As a result, the BRAS function SHOULD_[128] be located as close to the access node as possible from an ATM hop perspective. The daisy chaining SHOULD NOT_[129] exceed a depth of more than two ATM switching/multiplexing points in the Access Node. Additionally, if the BRAS does not include ATM switching functions, then an additional layer of hierarchical scheduling MUST_[130] be used to manage the trunk to the ATM switch.

The BRAS function MAY_[131] be integrated into the access node, however one of the constraints of this architecture is that it must account for a large embedded base of access nodes that do not support this function.

In order to preserve an IP flow's characteristics, the customer CPE MUST_[132] be involved in the QoS architecture. This is especially true when dealing with upstream traffic. This connection is typically the slowest link, and the most likely link to incur congestion and add delay and jitter within the service. To maintain fair but effective throughput over this link the RG MUST_[133] support packet classification and scheduling in accordance with DiffServ. The RG MUST_[134] also support a method of minimizing latency for EF traffic (e.g. fragmentation or MTU adjustment) that minimizes overhead, especially at times when no EF traffic is present.

The typical DSL customer is connected to the Regional/Access Network via a single ATM AAL5 PVC. This single PVC should be leveraged to the extent possible using the capabilities described above. Although the target architecture to support QoS enabled IP services seeks to utilize a single ATM AAL5 PVC per CPN, it is recognized that certain required network element features identified in this document have yet to be developed. In particular, dynamic packet fragmentation/MTU sizing in the CPE (needed to control jitter and delay for short packet/high priority applications) may trail the availability of other required network element features. In order to meet the demands of service descriptions previously identified in an acceptable timeframe, a second ATM PVC

MAY_[135] be provisioned as an interim solution to provide a means to separate those application flows having tight jitter and latency requirements. This second PVC will require that DSL modems support multiple PVCs. For the service model proposed in this document, the number of PVCs per customer SHOULD NOT_[136] exceed 2.

To support bandwidth on demand products or other differentiated services that implicitly require additional bandwidth on demand, a subscriber's access sessions MUST_[137] be shaped and policed by the BRAS and RG instead of permitting cell insertion at the DSL line rate. This change is accompanied by changing the ATUs to allow them to synchronize at or near their maximum rate. Since this architecture allows for multiple simultaneous access sessions, it MUST_[138] also be possible to independently modify the shapers and policers on each session. The policy data for the classification and shaping of traffic at the RG is provided at service configuration and is not a real time capability. The policy data for the classification and shaping of traffic at the BRAS can be provided at service configuration or may be dynamically configured.

Phase one assumes that the Regional/Access Network provider has established an IP-based architecture similar to that shown in Figure 4. This figure can be combined with Figure 2 in order to support the end-to-end view of the QoS-enabled network that follows. That combination is presented in Figure 20.

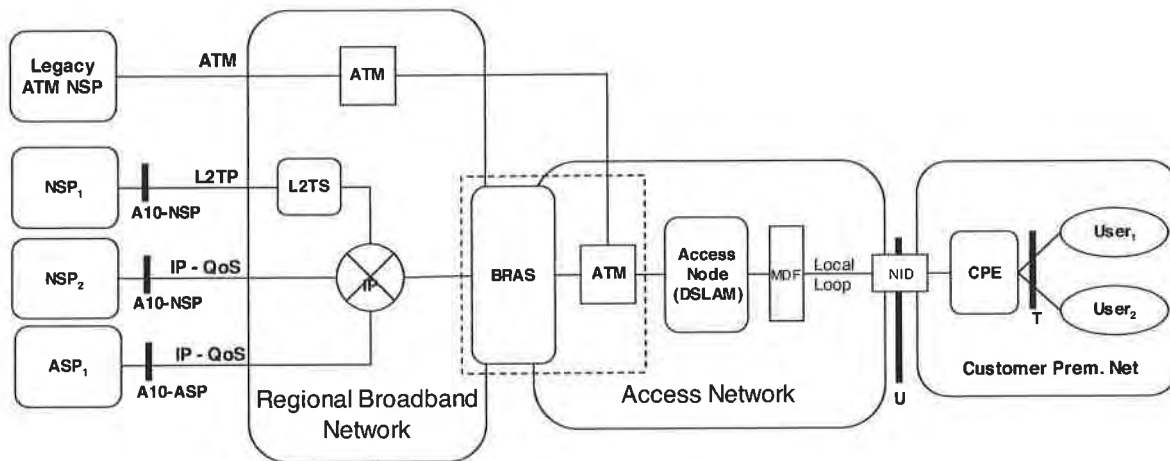


Figure 20 – QoS-enabled Network Topology

The two critical points where IP-QoS is managed are the BRAS and the CPE (RG). Intervening elements (like DSLAMs) are not envisioned to become layer-3 routers, and this architecture assumes that they will not be layer-3 aware when they manage congestion. This arrangement supports multiple business relationships and provides connectivity for various users to access various services without requiring all services to be provided by a single provider.

Phase 1 is characterized by Diffserv provided through static provisioning. Phase 2 describes a subsequent time with a dynamic mechanism for changing the Diffserv QoS parameters through the use of a policy-based networking enhancement.

Phase 1

Assumptions:

- In this phase there will be multiple BE NSP connections with few (1 or 2) EF sessions for real time applications (voice, Video conferencing). There will be little or no AF traffic – as applications would have to make use of static pre-configured AF classes rather than requesting one that suits the application.
- For phase 1 it is assumed that only one EF application per subscriber need be supported at a time (user performs the CAC across real-time applications). Within an application domain it is the application's responsibility to perform the CAC.
- Classification is performed at the RG on a session basis or accepted via markings attached to packets by the CPE

- Performing dynamic, per-application classification requires a 5-tuple classifier to be pushed down to the RG and is not likely in the short term.
- The DSLAM modems are allowed to sync near or at the max rate both upstream and downstream.
- Hierarchical scheduling is performed at the BRAS to provide IP QoS congestion mechanisms for the downstream path. Similar policing is performed in the upstream path.
- Packet-by-packet QoS requires being in the PTA (or bridged 2684) model at a given element.

Characteristics:

- Multi-user multi-destination is supported
- IP QoS is managed at the RG and BRAS
- The RG and BRAS are configured with common set of traffic profiles
- RG is configured by manufacturer or during installation (install CD)
- Statically assigned BE and EF queues will be supported in the RG.
 - Optional are statically assigned AF queues that could support 3 or 4 popular streaming arrangements or potential Gold/Silver/Bronze services. This option will require defining Diffserv classes that will be applicable across envisioned future services.
- Profile information defines the rate to which traffic should be shaped and the queuing behavior that should be used.
- Profile information will also determine the valid DSCPs.
- A small number of shaping profiles will be defined for the various connection speeds (e.g. 1.5x265; 1.5x384; 384x384; 768x512)
- Sessions are individually shaped based on profile and share the aggregate DSL sync rate. If the total BW per profile exceeds the available sync rate then the traffic shares the BW in a "fair" manner among similar QoS service classes.
- If the RG initiated the session, and it is authenticated, then it is told which pre-provisioned profile to use. Various potential protocols and mechanisms to do this have been discussed at the DSLF. Note, if a CPE device behind the RG initiates a PPPoE session then it remains PPPoE through the RG, and is BE traffic by definition. (Even if it becomes a PTA connection at the BRAS)
- In either a PTA or L2TP model the BRAS will police traffic in the upstream direction and shape traffic in the downstream direction.
- BRAS shaping, policing, and marking is done on a per session basis, not per application. However, the diffserv queues can be arranged within an access session so that various aggregate service classes can be provided to applications that indicate which class of service they desire. The application needs to set the DSCP properly in order to make use of this function.
 - An end-to-end PPP session is given a uniform QoS treatment, but can be shaped (e.g. 1.5x256).
 - A single, additional PPP or 1483 session is used to access the ASP network.
- The BRAS profiles are updated through provisioning, not signaling, and may be indicated via RADIUS.
- New profiles are added/updated in the RG by the customer manually configuring the device or by downloading a new software image

5.3.2 Phase 2 QoS Mechanisms

As previously mentioned, Phase 2 is adds a dynamic mechanism for changing the Diffserv QoS parameters through the use of a policy-based networking.

Assumptions:

- Builds on the capabilities in phase 1.
- This phase enhances the granularity of the classification and population of policies in the BRAS and RG.
- Multiple sessions to multiple destinations, each with multiple applications that may require different QoS treatment

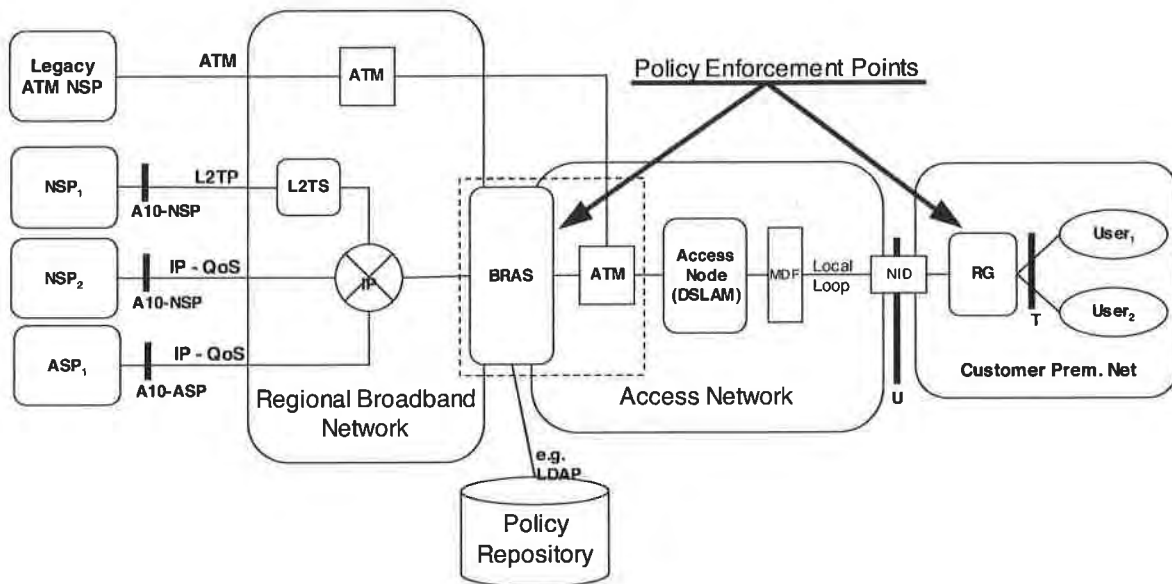


Figure 21 – Phase 2 with Policy-based profiles

Characteristics:

- When an NSP access session is authenticated the NSP MAY provide a profile indicator associated with that session in its response to the BRAS.
- Once the BRAS receives the profile indicator, it retrieves the full profile from the Policy Repository. Similarly, information is sent to the RG when it requests a profile. This step allows coordination among NSP and ASP profiles. Note also, that for some policy functions, the policy repository may be co-resident with the BRAS or RG.
- No single ASP authenticates the ASP access session, so a profile for that session is put together by the Policy Repository and is based on various ASP subscriptions associated with that access session.
- ASPs can update the profile either through subscription or through a dynamic protocol, like LDAP.
- Subscription profile information as well as DSL sync rate and user preferences are stored in the Policy Repository and accessed using a protocol, like LDAP.
- A policy manager is responsible for managing potentially conflicting ASP and NSP profiles and subscriptions and also creates billing data for services.
- The profile is populated in the elements in near-real time (no reset or “reboot” required).
- Diffserv marking and queuing behavior on RG is performed on 5-tuple matching (SA, DA, SP, DP, PI) as well as the mapping of existing marks and access sessions into various “equivalent” classes. For example, PPPoE access through a RG will continue to be given BE treatment.

5.3.2.1 Diffserv Requirements**RG**

The RG requirements below only apply to the support of IP-QoS and should not be mistaken as a complete list of RG requirements needed in order to support this architecture.

The RG SHOULD_[139] be the central point for controlling traffic within the customer premises and traffic destined for the Access Network.

The RG MUST_[140] support Diffserv marking and remarking in accordance with IETF RFC 2474.

The RG MUST_[141] support Diffserv queuing for the Assured Forwarding (AF) and Expedited Forwarding (EF) classes in accordance with IETF RFC 2597 and IETF RFC 3246 for carrying real time traffic. The exact AF classes supported and behaviors will be described in a future document.

The RG MUST_[142] support multiple queues with the appropriate scheduling mechanism to effectively implement Diffserv queuing behaviors (e.g. strict priority, Weighted Fair Queuing).

The RG MUST_[143] be configured with the classification parameters for mapping traffic into a given Diffserv Per Hop Behavior (PHB) during service configuration.

The RG MUST_[144] support the capability to fragment AF and BE traffic in order to constrain the perturbing impact of AF and BE packets on EF traffic delay, for example using a mechanism such as MLPPP LFI [RFC1990].

The method of minimizing latency for EF traffic SHOULD_[145] minimize overhead, especially at times when no EF traffic is present.

If multiple PVCs are provisioned at the ATU-R, the RG MUST_[146] support the mapping between a Diffserv Code Point (DSCP) (low latency queue) and a specific PVC. (Using a PVC bundle is the desired way to meet this requirement.)

BRAS

The BRAS MUST_[147] support Diffserv marking and remarking in accordance with IETF RFC 2474.

The BRAS MUST_[148] be able to police the use of DSCPs received from customer traffic and remark traffic if it does not match the customer profile data – including potentially dropping unauthorized traffic.

The BRAS MUST_[149] support Diffserv queuing for the Assured Forwarding (AF) and Expedited Forwarding (EF) classes in accordance with IETF RFC 2597 and IETF RFC 3246. The exact AF classes supported will be described in a future document. These queues are defined within the context of the DSLAM connectivity between the BRAS and the access node in affect managing the access node's downstream bandwidth.

The BRAS MUST_[150] support multiple queues per user with the appropriate scheduling mechanism to effectively implement Diffserv queuing behaviors (e.g. strict priority, Weighted Fair Queuing).

The BRAS MUST_[151] support the mapping of DSCP to MPLS LSP, VLAN, ATM VP, or other traffic engineering capabilities in the Regional Network.

The BRAS MUST_[152] support the capability to fragment AF and BE traffic in order to constrain the perturbing impact of AF and BE packets on EF traffic delay, for example using a mechanism such as MLPPP LFI [RFC1990].

The method of minimizing latency for EF traffic SHOULD_[153] minimize overhead, especially at times when no EF traffic is present.

If multiple PVCs are per subscriber are provisioned, the BRAS MUST_[154] support the mapping between a Diffserv Code Point (DSCP) and a specific PVC. (Using a PVC bundle is the desired way to meet this requirement.)

5.3.2.2 Traffic Engineering Requirements

In order for the BRAS to effectively manage downstream IP traffic through layer 2 devices using the hierarchical scheduling model, the BRAS MUST_[155] have awareness of all the traffic that is traversing those layer 2 elements. This can be accomplished in 2 ways. The first and most straightforward method is for all traffic destined for the access node to flow through the BRAS enabling it to manage the traffic accordingly. In this case the hierarchical scheduling model in the BRAS will be based on the full downstream trunk bandwidths and DSL synch rates. In cases where not all traffic flows through the BRAS, the resources that are not under the control of the BRAS MUST_[156] be subtracted from the resources that the BRAS manages. The remainder of the resources on the trunks and DSL lines will be managed using the hierarchical scheduling model. The traffic that is not under the control of the BRAS MUST_[157] be traffic engineered in a way that it cannot consume resources that the BRAS is controlling. Engineering around the BRAS incurs risk and must be done with care.

5.3.2.3 Admission Control

End-to-end QoS admission control is not required in this phase. Admission control for access network QoS (bandwidth on demand) is required. Application layer admission control will be predicated on service specific

resources (such as availability of logical ports on servers and their knowledge of network topology). Furthermore, admission control may be provided in the provisioning aspect of a QoS policy.

6 SERVICE LEVEL MANAGEMENT

6.1 Introduction

Service Level Management is intended to provide 3 levels of benefit – increasing over time:

- To provide a list of the salient network performance and operational metrics that might be used in a Service Level Objective (SLO) or Service Level Agreement (SLA).
- To provide a standard definition of such metrics so that its meaning would be common when used by various providers.
- To provide extreme values that are driven by architectural considerations where applicable. For example, while it is NOT the intention of this document to set the SLO or SLA for Network Delay (Latency), any network that purports to support Voice over IP (VoIP) will need to have a maximum delay that is within the bounds necessary to support VoIP.

6.2 Network Performance Metrics

1. **Network Availability** - The percent of time that the Regional/Access Network is available for subscribers to connect. This metric is defined on some time basis, such as a month, a week, or a year. An SLA should also specify not the entire network but the section of the network for which the Regional/Access Network Provider is responsible. For example, the Regional/Access Network Provider is not responsible for NSP problems.
2. **Network Delay (Latency)** – The time it takes for a data packet to traverse the Regional/Access Network, from end-to-end or edge-to-edge. Latency is defined in milliseconds and can be a one-way or round-trip delay.
3. **Message Delivery** - The ability of the Regional/Access Network to transmit traffic at the negotiated speed. Some applicable measurements are packet loss). These metrics must have a time base as well.
4. **Network Jitter** – The variance of network latency. Jitter is defined in milliseconds.

6.3 Operational Metrics

1. **Mean Response Time** - The time it takes the Regional/Access Network Provider to respond to submitted reports of trouble
2. **Mean Time to Restore Service** – The measurement of the Regional/Access Network Provider's ability to restore service within the negotiated interval
3. **Ordering System Reliability** – The measurement of the consistent availability of ordering system.
4. **End-User Installation Guarantee** – The measurement of the Regional/Access Network Provider's ability to meet negotiated order due dates.

7 SERVICE MANAGEMENT

The architecture proposed in this document clearly needs management systems to provide the controls necessary to support the underlying service “building blocks”. The following lists are examples of new data points that management systems MUST_[158] support. Network elements and Service Providers will use these new data elements for service provisioning and data delivery. It is expected that the Operations and Network Management working group of the DSL Forum will provide contributions to augment this section.

7.1 Subscribers

Because of the changes in how DSL is provisioned and managed, there are a number of new data points that MUST_[159] be tracked for each subscriber. Among these are:

- Maximum sustainable subscriber bandwidth
- Maximum number of sessions allowed
- Permitted destinations
- Default protocol
- Default destination
- Default bandwidth
- Single host or subnet needed
- Restricted subscriber (single destination only)
- Total reserved bandwidth

7.2 Service Providers

Because of the changes in how DSL is provisioned and managed, there are more details needed per Service Provider. When various choices listed for an option, these are to be considered as examples only and not a definitive list of the choices for a given option.

- Minimum bandwidth needed
- Minimum QoS level
- Various protocol metrics
- Subscriber protocol (IP, PPPoE)
- Protocol (IP, L2TP, ATM)
- Authentication
- IP address assignment
- Transport
- Maximum simultaneous sessions

GLOSSARY

AAA	Authentication, Authorization, and Accounting
AAL5	ATM Adaptation Layer 5
ADSL	Asymmetric Digital Subscriber Line
AF	Assured Forwarding
API	Application Program Interface
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
ATMARP	ATM Address Resolution Protocol
ATMF	ATM Forum
ATU-C	Access Termination Unit - Central Office (at Access Network end)
ATU-R	Access Termination Unit - Remote (at customer end)
B-NT	Broadband Network Termination
BE	Best Effort
BGP	Border Gateway Protocol
BoD	Bandwidth on Demand
BRAS	Broadband Remote Access Server
CBR	Constant Bit Rate
CO	Central Office
COPS	Common Open Policy Service
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSP	Corporate Service Provider
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiate Services
DLC	Digital Loop Carrier
DNS	Domain Name Service
DS1	Digital Signal level 1 (1.544 Mbps)
DSCP	Differentiated Services (Diffserv) Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EF	Expedited Forwarding
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GFR	Guaranteed Frame Rate
iBGP	internal Border Gateway Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Secure Internet Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Technical
L2TP	Layer 2 Tunneling Protocol
L2TS	Layer 2 Tunnel Switch
L2oMPLS	Layer 2 over MPLS
LAC	Layer 2 Access Concentrator
LAN	Local Area Network
LD	Long Distance
LDAP	Lightweight Directory Access Protocol
LER	Label Edge Router
LLC	Logical Link Control

LSP	Label Switched Path
LNS	L2TP Network Server
MAC	Medium Access Control
MARS	Multicast Address Resolution Server
MASS	Multi-Application Selection Service
MBGP	Multicast Boarder Gateway Protocol
MPEG	Motion Pictures Expert Group
MPLS	Multi-Protocol Label Switching
MS/MD	Multi Session / Multi Destination Service
MTU	Message Transfer Unit
NAPT	Network Address Port Translation
NG-DLC	Next Generation Digital Loop Carrier
NHRP	Next Hop Resolution Protocol
NSP	Network Service Provider
OC3	Optical Carrier 3
OSPF	Open Shortest Path First
PC	Personal Computer
PHB	Per Hop Behavior
PHY	Physical Layer
POP	Point of Presence
POS	Packet over SONET
PPP	Point-to-Point Protocol
PPPoA	Point-to-point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PTA	PPP Terminated Aggregation
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAM	Remote Access Multiplexer
RFC	Request For Comments
RG	Routing Gateway
RRP	Resource Request Protocol
RSVP	ReSource reserVation Protocol
RT-DSLAM	Remote Digital Subscriber Line Access Multiplexer
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLO	Service Level Objective
SNAG	Service Network Architecture Group (DSL Forum)
SONET	Synchronous Optical Network
SVC	Switched Virtual Circuit
TCP	Transmission Control Protocol
TE	Traffic Engineering
TR	Technical Report (DSL Forum)
TV	Television
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
VBR-nrt	Variable Bit Rate - non-Real Time
VBR-rt	Variable Bit Rate - Real Time
VC	Virtual Circuit
VCC	Virtual Circuit Connection
VLAN	Virtual Local Area Network
VoD	Video on Demand
VP	Virtual Path
VPC	Virtual Path Connection
VPN	Virtual Private Network

VoBB	Voice over Broadband
VoIP	Voice over Internet Protocol
WFQ	Weighted Fair Queuing

APPENDIX A REFERENCES

- [1] DSL Forum TR-010, "Requirements & Reference Models for ADSL Access Networks: The "SNAG" Document"
- [2] DSL Forum TR-025, "Core Network Architecture for Access to Legacy Data Networks over ADSL"
- [3] DSL Forum TR-032, "CPE Architecture Recommendations for Access to Legacy Data Networks"
- [4] DSL Forum TR-037, "Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM"
- [5] DSL Forum TR-042, "ATM Transport over ADSL Recommendation (Update to TR-017)"
- [6] DSL Forum TR-043, "Protocols at the U Interface for Accessing Data Networks using ATM/DSL"
- [7] M. Kaycee, G. Gross, A. Lin, A. Malis, J. Stephens, "PPP over AAL5," IETF RFC 2364, July 1998
- [8] Skwoler, et. al, "The PPP Multilink Protocol (MP)," IETF RFC 1990, August 1996
- [9] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF RFC 2474, December 1998.
- [10] L. Mamakos, et al, "A Method for Transmitting PPP Over Ethernet", IETF RFC 2516, February 1999
- [11] D. Grossman, J. Heinanen, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", IETF RFC 2684, September 1999
- [12] W. Townsley, et al, "Layer Two Tunnelling Protocol (L2TP)" IETF RFC 2661, August 1999
- [13] J. Heinanen, R. Guerin, "A Single Rate Three Color Marker" IETF RFC 2697, September 1999
- [14] J. Postel, J.K. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", IETF RFC 1042, February 01, 1988.
- [15] S.E. Deering, "Host extensions for IP multicasting", IETF RFC 1112, August 01, 1989.
- [16] W. Fenner, "Internet Group Management Protocol, Version 2", IETF RFC 2236, November 1997.
- [17] T. Bates, Y. Rekhter, R. Chandra, D. Katz, "Multiprotocol Extensions for BGP-4", IETF RFC 2858, June 2000.
- [18] K. Nichols, S. Blake, F. Baker, D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF RFC 2474, December 1998.
- [19] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski., "Assured Forwarding PHB Group", IETF RFC 2597, June 1999.
- [20] D. Black, S. Brim, B. Carpenter, F. Le Faucheur, "Per Hop Behavior Identification Codes", IETF RFC 3140, June 2001.
- [21] B. Davie, A. Charny, J.C.R. Bennet, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", IETF RFC 3246, March 2002.
- [22] D. Grossman, "New Terminology and Clarifications for Diffserv", IETF RFC 3260, April 2002.
- [23] The ATM Forum "Traffic Management Specification Version 4.1", AF-TM-0121.000, March 1999.

APPENDIX B Informative Example of Queuing Architectures for RG and BRAS

B.1 Example Queuing Architecture for RG

The queuing and scheduling discipline envisioned upstream for the RG is shown in Figure 24.

There are multiple access sessions supported in this model, however, all traffic is classified and scheduled in a monolithic system. So, while it might appear at first that the Diffserv queuing and scheduling might apply only to IP-aware access – in fact all access, IP, Ethernet, or PPP is managed by the same system that adheres to the Diffserv model.

For example, at the bottom of the figure, BE treatment is given to the non-IP-aware access sessions (PPPoE started behind the RG or delivered to an L2TP tunnel delivery model). This queue might be repeated several times in order to support fairness among multiple PPPoE accesses – or it may be a monolithic queue with separate rate limiters applied to the various access sessions.

The PTA access is a single block of queues. This is done because NSP access typically works with a single default route to the NSP, and managing more than one simultaneously at the RG would be perilous. The Σ rate limiter would limit the overall access traffic for a service provider.

Rate limiters are also shown within the EF and AF service classes because the definition of those Diffserv types is based on treating the traffic differently when it falls into various rates.

Finally, at the top of the diagram is the ASP access block of queues. In phase 1A, these queues are provisioned and provide aggregate treatment of traffic mapped to them. In phase 1B, it will become possible to assign AF queues to applications to give them specific treatment instead of aggregate treatment. The EF service class may also require a high degree of coordination among the applications that make use of it so that its maximum value is not exceeded.

Notable in this architecture is that all the outputs of the EF, AF, and BE queues are sent to a scheduler (**S**) that pulls traffic from them in a strict priority fashion. In this configuration EF traffic is, obviously, given highest precedence and BE is given the lowest. The AF service classes fall in-between.

Note that there is significant interest in being able to provide a service arrangement that would allow general Internet access to have priority over other scavenger class (bulk rate) services.¹ Such an arrangement would be accomplished by assigning the bulk rate service class to BE and by assigning the default service class (Internet access) as AF with little or no committed information rate.

Given this arrangement, the precedence of traffic shown in the figure is arranged as:

1. EF – red dotted line
2. AF – blue dashed line (with various precedence among AF classes as described in RFC2597)
3. BE – black solid line

¹ This “bulk rate” scavenger class service would typically be used for background downloads and potentially for peer-to-peer applications as an alternative to blocking them entirely.

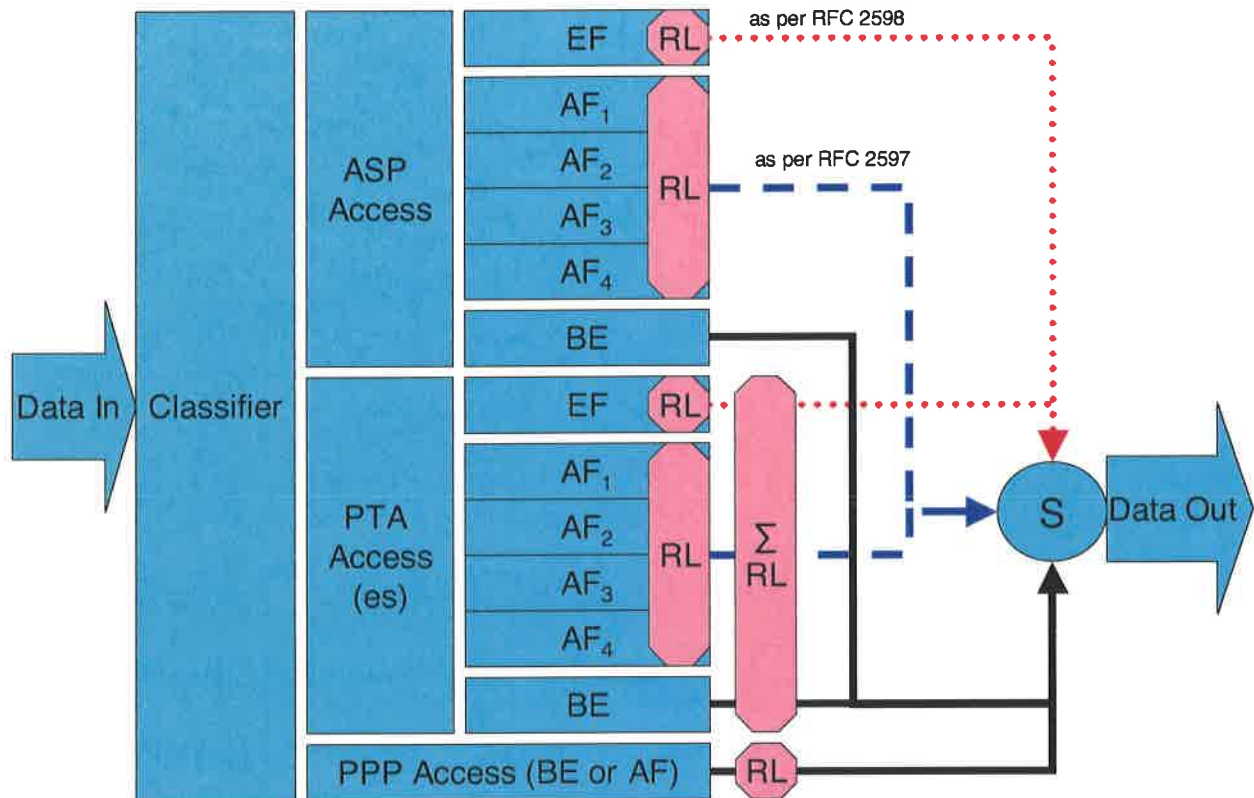


Figure 22 – Queuing and Scheduling Example for RG

In Figure 22 the following abbreviations apply:

- ASP – Application Service Provider
- PTA – PPP Terminated Aggregation
- PPP – Point-to-Point Protocol
- EF – Expedited Forwarding – as defined in RFC 3246
- AF – Assured Forwarding – as defined in RFC 2597
- BE – Best Effort forwarding
- RL – Rate Limiter
- ΣRL – Summing Rate Limiter (limits multiple flows)
- S – Scheduler

B.2 Example Queuing Architecture for a BRAS that can also switch ATM

An example of a queuing and scheduling discipline for a BRAS that meets the hierarchical shaping/scheduling requirements envisioned downstream is shown in Figure 24. Note that in this example, the BRAS is also an ATM switch, although the ATM switching capability is not essential for all BRAS designs.

There are multiple access sessions supported in this model, however, all traffic is classified and scheduled in a monolithic system. So, while it might appear at first that the Diffserv queuing and scheduling might apply only to IP-aware access – in fact all access, IP, Ethernet, PPP, and even ATM is managed by the same system that adheres to a combination of queuing disciplines taken from ATM and the Diffserv model. Note that the ATM disciplines are for backward compatibility, and don't otherwise interact with the Diffserv disciplines.

The BRAS will need to provide a congestion management function that will allow the synthesis of IP QoS through downstream elements that are not QoS aware. Accomplishing this is envisioned as a marriage of IP and ATM technologies with ATM and WFQ scheduling performed against diffserv and ATM queues. At a very high level, the queuing architecture desired for the BRAS can be described as IP DiffServ classification and queues mated to a slightly enhanced ATM scheduler. This results in emitting (shaping) ATM cells into the downstream network according to their VC contracts and ATM traffic engineering requirements, and so that no congestion occurs on the downstream links and systems. The result is that congestion queues in the BRAS, and eventual data discard occurs in packets being dropped from the DiffServ queues according to their precedence.

Figure 23 is provided as a reference to reinforce the problem and to provide exemplary infrastructure to show how the queuing system works.

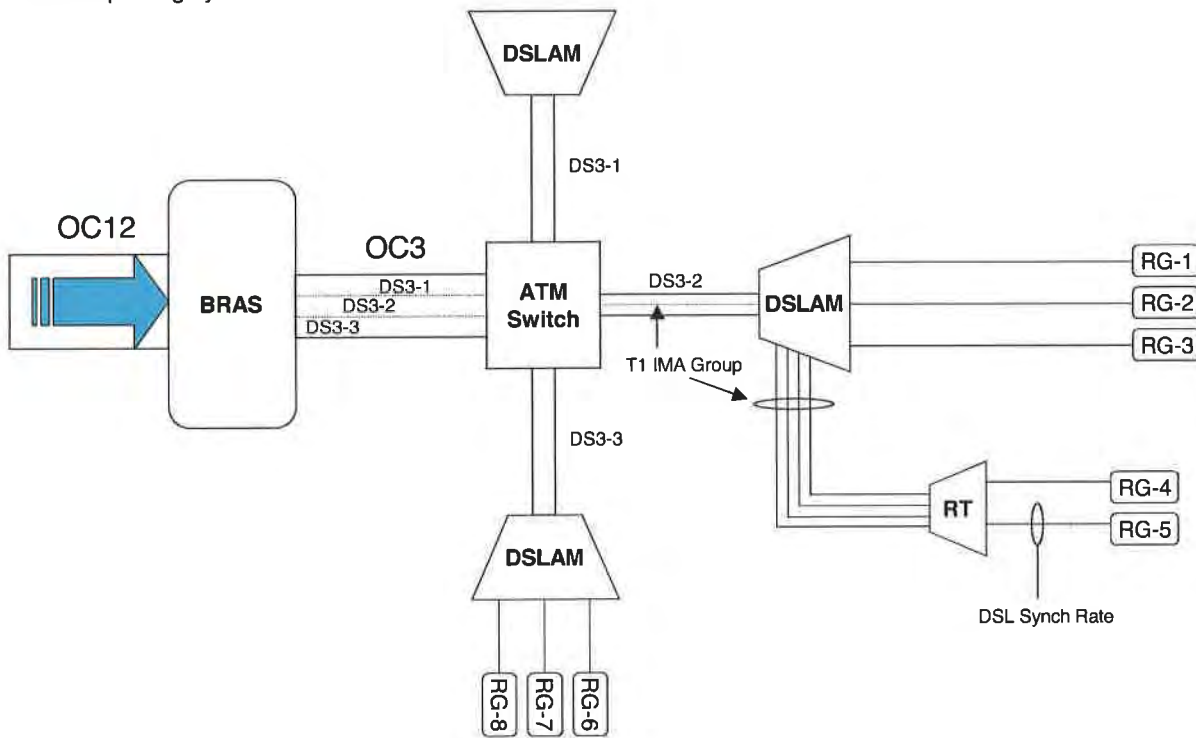


Figure 23 – Reference Topology for Queuing and Scheduling Example for a BRAS that can also switch ATM

In this example the BRAS is on the left and uses a central ATM switch to multiplex access to 3 DSLAMs, at the top, right, and bottom. The DSLAM on the right has an additional RT unit daisy-chained behind it using a T1 IMA group. Various RGs are behind the ADSL lines at differing sync rates. As stated earlier in this TR, there is an assumption that congestion in this network never occurs in the fabric of the ATM switch, DSLAMs, or RT units, and always occurs through the over-subscription of transport links. In this example, those links would be:

- 1) OC 3 between BRAS and ATM switch
- 2) DS3 between ATM switch and DSLAMs
- 3) T1 IMA between DSLAM and RT
- 4) DSL loop to the RGs

Now, we observe traffic entering the BRAS and its queuing discipline, and see the following:

- 1) First, traffic is classified in a similar way to what was described for the RG. One notable exception being legacy ATM traffic, which is queued according to the class associated with the VC.

- 2) It is then policed, or rate limited, according to the services associated with the queues (if any). Again with an ATM exception of applying ATM-appropriate disciplines, such as CBR, VBR or UBR.

Traffic remains in the queues until it is scheduled for delivery. If congestion would occur in the BRAS or on a downstream link, then the queues for that traffic fill according to their discipline.

- 1) The scheduler is best described in reverse. First, the egress port of the BRAS is scheduled to the port rate (OC3 in this example). At this level, the scheduler is set for a WFQ algorithm, weighted according to the data rates of the VPs that are scheduled. Traffic is "pulled" from the subordinate schedulers in priority (as described for the RG scheduler) but with the limitations set by the various subordinate schedulers.
- 2) Then each ATM VP is scheduled. In this case there are 3 DS3 VPs that each lead to a different DSLAM and are scheduled to the DS3 rate. The schedulers are set to work in a similar way to the egress port scheduler.
- 3) In a departure from a typical ATM device, an additional layer of hierarchy is defined for "groups" of VCs in order to account for bandwidth constraints beyond the DSLAM. This can occur with DLC-based and RT-based DSLAMs that typically use IMA groups daisy-chained into Co-based DSLAMs. In this example, the VC Group Scheduler accounts for the T1 IMA group to the RT.
- 4) The next stage is the scheduler for the ATM VC. This scheduler works almost exactly like the RG. In the (optional) case where 2 PVCs are used the bandwidth of the DSL line is divided between the 2 PVCs instead of being directly assigned.
- 5) Finally, the queues within a given access session are scheduled to a maximum rate assigned to the access session. Initially static, the limit eventually becomes profile-driven through the policy repository.

As was described for the RG queuing architecture, all the outputs of the EF, AF, and BE queues are sent to a (hierarchical) scheduler (S) that pulls traffic from them in a strict priority fashion. Similar to the description of the RG queuing, a configuration may create the opportunity to establish access types with a lower priority than existing Internet access.

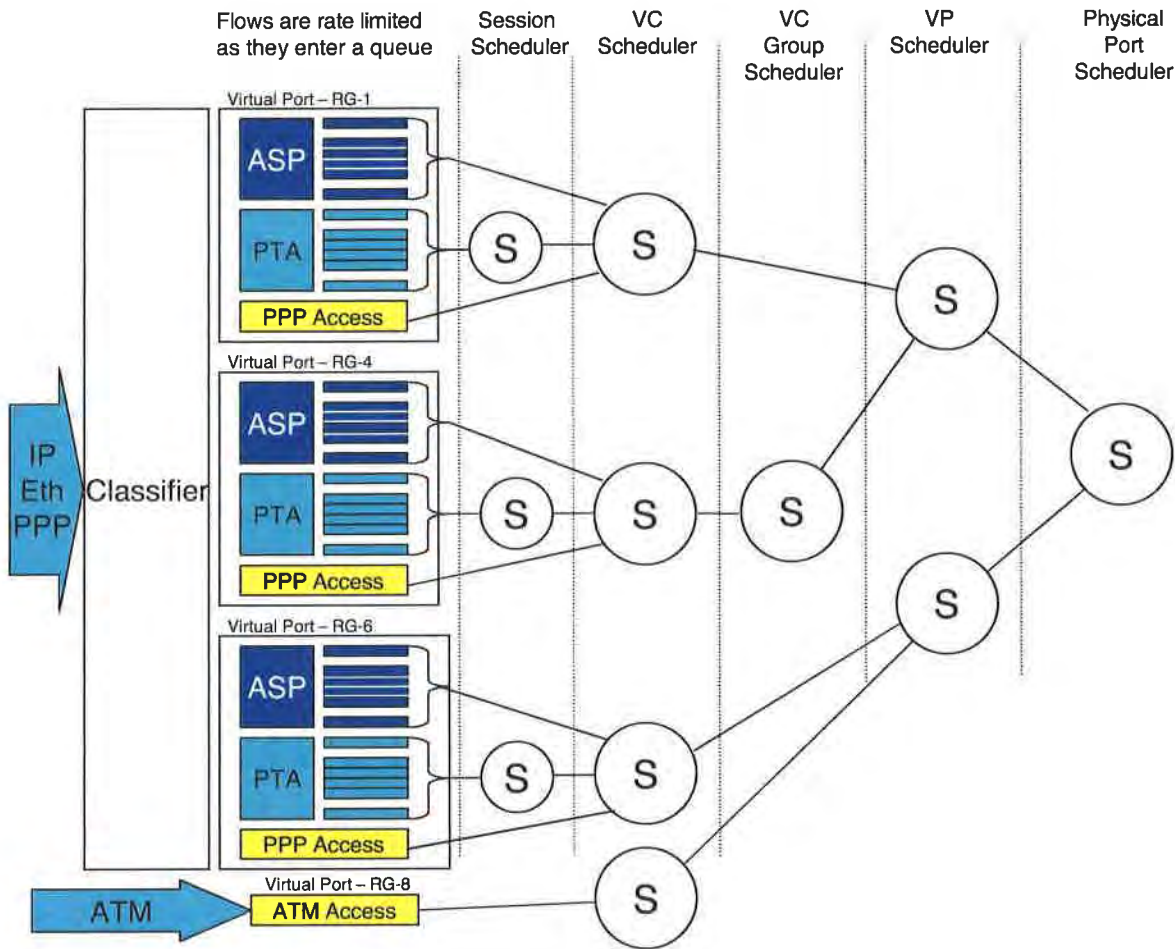


Figure 24 – Queuing and Scheduling Example for a BRAS that can also switch ATM

In Figure 24 the following abbreviations apply:
 ASP – Application Service Provider
 ATM – Asynchronous Transfer Mode
 PTA – PPP Terminated Aggregation
 PPP – Point-to-Point Protocol
 S – Scheduler

APPENDIX C Informative Appendix on Signaled QoS

This appendix captures the concepts and planning for a potential follow-on signaled QoS mechanism. While it is uncertain that this phase will be required, concepts are brought forward to provide a perspective of how it would interact with the QoS mechanisms defined in this specification. The exact signaling protocol remain an item of debate, so this section refers to it with the abstract term Resource Reservation Protocol (RRP) and collects attributes that are likely to become requirements when the protocol becomes defined.

C.1 Signaled QoS Mechanisms

The architecture for additional QoS enhancements is introduced in this section. This section is included for illustrative purposes and may be further defined in future documents.

Signaled QoS adds per IP flow resource reservation capabilities in the Regional/Access Network. This step continues to leverage the RG and BRAS as the IP QoS managers of the access network. Rather than simply managing the aggregate scheduling of Diffserv resources, the BRAS will be able to perform per flow admission control ensuring that resources are never over-booked. Diffserv aggregate traffic treatments may continue to be used beyond the BRAS toward the regional network for scalability reasons. Keeping per flow resource reservation limited to the access portion of the Regional/Access Network could limit scalability/performance issues known with prior end-to-end reservation schemes.

In this phase:

- Applications, located in any of the reference networks, request service or resources of the Regional/Access network (e.g. through RRP).
- The RG and BRAS are involved in requests for services and resources in the network based on a per-application need (e.g. they monitor or proxy RRP messages).
- The BRAS acts like an RSVP border proxy and queries the policy repository. It responds based on the network availability of traffic engineered resources (MPLS – TE, ATM VP, etc) and customer profile.
- QoS service profiles can be applied to the BRAS and RG based on the requested application need.

C.1.1 Signaled QoS Assumptions

BRAS

The BRAS may support a RRP for the assignment of resources. When resources are not available at any point under its control the BRAS would reject the request and provide feedback to the initiating host.

The BRAS would need to know the DSL sync rates of the ATU-Rs that are connected to the access nodes that it manages. Based on a given ATU-R's DSL synch rate and customer profile the BRAS would manage the admission of sessions to that customer premises. An external policy/management server could feed this information to the BRAS.

The BRAS might intercept RRP and other application layer (e.g. SIP) messages that are not addressed to it and use these messages in making admission decisions.

The BRAS would support mapping reservation requests into Diffserv PHBs and managing the PHBs as reservable resources.

CPE

The CPE assumptions below only apply to the support of differentiated services.

The CPE requesting differentiated services could be integrated with the ATU-R. Non-integrated CPE devices will also be supported (e.g. IP Phones, PC running video conferencing software, set top boxes, etc).

The CPE would need to support IP layer signaled QoS via a RRP. These messages would be addressed to the destination host and not to the BRAS.

The CPE would not make any admission decisions.

C.1.2 Diffserv Assumptions

BRAS

The BRAS will accept policy information regarding how to manage Diffserv signaled flows from an external entity.

CPE

If the signaling messages indicate the DSCP to be used by a session requesting access, the CPE would then use the specified DSCP.

The CPE will also accept policy information regarding how to manage Diffserv signaled flows from an external entity.

C.1.3 Traffic Engineering Requirements

The RRP mechanism described only has resource knowledge of the local access network and does not have an end-to-end picture of the connection. As a result, the interconnection network within the Regional/Access Network (beyond the BRAS) would be engineered to provide support for enhanced services in aggregates. It is expected that within the core of the Regional/Access Network that aggregate traffic engineering techniques can efficiently serve the needs of enhanced applications.

C.1.4 Admission Control

Per-flow admission control is envisioned at the BRAS. Admission decisions are made based on resource availability AND subscriber profile data. Both of these parameters could be sent to the BRAS via an external policy/provisioning server.

Application level admission control can also be applied in addition to the network based admission control.

EXHIBIT A

http://web.archive.org/web/20050131044258/http://www.dslforum.org/aboutdsl/Technical_Reports/TR-068.pdf

TECHNICAL REPORT

DSL Forum

TR-068

Base Requirements for an ADSL Modem with Routing

May 2004

Produced by:

DSLHome-Technical Working Group

Editor: Barbara Stark, BellSouth

Working Group Co-Chairs:

Greg Bathrick, Texas Instruments

George Pitsoulakis, Westell

Abstract:

This Working Text will specify requirements for an ADSL modem with embedded router functionality that can be deployed through retail stores and then configured for customer use by service providers. These requirements will lead to retail devices that can provide customers with consistent features, connectivity and operation.

These requirements are both backward and forward-looking. They attempt to address the needs of current DSL services and architectures as well as starting to address future needs. Some requirements have been included in support of TR-059. However, these requirements do not fully complement the capabilities specified in TR-059.

Notice:

The DSL Forum is a non-profit corporation organized to create guidelines for DSL network system development and deployment. This Technical Report has been approved by members of the Forum. This document is not binding on the DSL Forum, any of its members, or any developer or service provider involved in DSL. This document is subject to change, but only with approval of members of the Forum.

©2003 Digital Subscriber Line Forum. All Rights Reserved.

DSL Forum technical reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only.

Notwithstanding anything to the contrary, the DSL Forum makes no representation or warranty, expressed or implied, concerning this publication, its contents or the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by the DSL Forum as a result of reliance upon any information contained in this publication. The DSL Forum does not assume any responsibility to update or correct any information in this publication.

Table of Contents

1	SCOPE AND PURPOSE.....	1
1.1	Scope.....	1
1.2	Requirements.....	1
2	MODEM REQUIREMENTS.....	2
2.1	Physical and Power.....	2
2.2	WAN: ADSL and ATM.....	6
2.3	Multiple PVCs.....	9
2.4	WAN: Access Protocols.....	9
2.5	LAN: Physical Interfaces.....	14
2.6	WAN and LAN: IP Addressing and DHCP Server.....	15
2.7	Routing and NAPT.....	20
2.8	Firewall.....	21
2.9	Naming Services.....	22
2.10	User Interface and Management.....	22
2.11	Graphical User Interface.....	29
2.12	Packaging.....	30
APPENDIX A	Application Level Gateway (ALG) and Port Forwarding List.....	31
APPENDIX B	Example Queuing for a DSL Router.....	34
APPENDIX C	Examples of Potential Configurations.....	36
C.1	Introduction.....	36
C.2	Basic DSL Modem as Router Initiating One or More PPPoE Sessions.....	36
C.3	“2684 Bridged” Mode.....	41
C.4	Simultaneous IP and PPPoE WAN Sessions.....	44
C.5	Single PC Mode of Operation.....	46
C.6	Router Embedded DHCP Server Gives Out Public IP Addresses (from use of IPCP extension).....	47

1 SCOPE AND PURPOSE

1.1 Scope

The document presents base requirements for an ADSL modem with embedded router functionality that can be deployed through retail stores and then configured for customer use by service providers. These requirements will lead to retail devices that can provide customers with consistent features, connectivity and operation.

These requirements specify a minimum set of features. It is expected that devices will include these in a superset of features (e.g., wireless, power line, 1394b, firewall, etc...).

These requirements are both backward and forward-looking. They attempt to address the needs of current DSL service and architectures as well as starting to address future needs. Some requirements have been included in support of TR-059, and are marked as [TR-059]. Any CPE that claims to be compliant with TR-059 must meet these requirements. It is understood that CPE that does not claim to be TR-059 compliant may not meet these requirements.

1.2 Requirements

In this document, several words are used to signify the relative importance of the specified requirements.

- MUST** This word, or the adjective “REQUIRED”, means that the definition is an absolute requirement of the specification.
- MUST NOT** This phrase means that the definition is an absolute prohibition of the specification.
- SHOULD** This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.
- MAY** This word, or the adjective “OPTIONAL”, means that this item is one which vendors may readily implement. Other modem features not identified in this document may also be implemented in the modem and are equivalent to the MAY value.

Throughout this document, the ADSL modem is referred to as “the device”. References to CPE indicate other equipment such as hosts including PC and workstations.

Requirements which are in support of TR-059 start with [TR-059].

Requirements which are specific to North America start with [North America].

2 MODEM REQUIREMENTS

2.1 Physical and Power

- I - 1 The device **MUST** be compact and have a physical profile suitable for desktop.
- I - 2 The device **SHOULD** be able to be wall mounted and stand on its side.
- I - 3 The device **MAY** have the ability to be mounted horizontally or vertically.
- I - 4 If wall mounted, the device **SHOULD** be oriented so that the cabling is routed toward the ground in order to reduce strain on the cabling.
- I - 5 A detachable wall-mounting bracket **MAY** be added to the device.
- I - 6 If the device can be wall mounted, specifications for screws and a template **SHOULD** be included with the device.
- I - 7 [North America] The device **MUST** be UL 60950 listed. This is the most recent replacement for UL 1950.
- I - 8 [North America] The device **MUST** display proof of CSA (Canadian Standards Association) or ULC (Underwriters Laboratories Canada) certification for CAN/CSA C22.2 No. 60950. This is the Canadian equivalent to and is identical to UL 60950.
- I - 9 [North America] The device **MUST** have the following electrical characteristics:
Voltage: 105 - 125 VAC @ 60 Hz
- I - 10 The power connector at the device **MUST** be securely connected to avoid accidental disconnect. This means that the connector **MUST** be either secured via a clip to the box or be held in place with significant force so that it does not readily pull out by minor pulling on the power cord.
- I - 11 [North America] If the power supply is external to the modem, it **MUST** be UL 1310 or UL 60950 listed and certified.
- I - 12 If the power supply is external to the device, it **SHOULD** be labeled with the DSL device vendor's name and the model number of the ADSL device.
- I - 13 If the power supply is external to the device it **SHOULD** be either small enough, or appropriately positioned on the power cord, so as not to block other power outlets.
- I - 14 If the power cable includes an analog to digital conversion brick, that brick **MAY** have a light on it.
- I - 15 The device **MUST** have an on/off switch. This switch **MUST** be positioned on the device in such a manner as to prevent accidental switching.
- I - 16 The Device **SHOULD** be tolerant of power fluctuations and brown-outs, continuing to operate normally and maintaining its configuration after these events.
- I - 17 If the on/off switch is labeled, it **SHOULD** be labeled "ON/OFF".
- I - 18 The device **MAY** be provided with a standby switch on the front, to stop or allow traffic to flow between WAN and LAN connections, without switching the device off and on.

- I - 19 The device **SHOULD** be able to detect faults and reset appropriately upon detection.
- I - 20 The device **MUST NOT** be USB powered.
- I - 21 The device **MUST NOT** use the local phone loop for power.
- I - 22 The device **MUST** have the following indicator lights:
 Power Ethernet DSL Internet
- I - 23 All physical ports and bridged connection types on the device (e.g., Ethernet, USB, Wireless, HomePlug, HomePNA, 1394, etc...) **MUST** have a link integrity indicator lamp on the device (1 per port if a separate physical port is present or per connection type if a separate port is not present).
- I - 24 [North America] The indicator lights **MUST** be labeled and in the order as indicated in I - 22 in a left to right or top to bottom orientation.
- I - 25 [North America] Port indicator lights not identified in I - 22 **MUST** be placed between the "Ethernet" and "DSL" lights and labeled (order and text) as identified in I - 23.
- I - 26 All port indicator lights **MUST** be located on the front of the device unless summary indicator lights are used.
- I - 27 Physical port indicator lights **MAY** be located next to the port and other than on the front of the device, so long as there is a summary indicator light for the associated interface type with the other port indicator lights on the front of the unit.
- For example, there may be Ethernet port indicator lights located on the back of the unit by each Ethernet connection as long as there is a summary indicator for the Ethernet connections on the front of the device in the standard location.
- I - 28 The indicator lights **MUST** be readily visible (99% human observer detection in less than 250 milliseconds) at 12 feet with an ambient illumination level of 550 foot-candles. Visibility **MUST** be maintained over a horizontal viewing angle of +/- 80 degrees and a vertical viewing angle of -20 to +45 degrees off the central axis.
- I - 29 When flashing, the indicator lights **MUST** flash at 4 Hz with a duty cycle of 50% (except as specified otherwise in this document).
- I - 30 The device **MUST** have a "On/Off" power indicator light. The power indicator **MUST** function as follows:
- | | | |
|-------------|---|---|
| Solid Green | = | Power on |
| Off | = | Power off |
| Red | = | POST (Power On Self Test) failure (not bootable) or
Device malfunction |

A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.

- I - 31 The device **MUST** have an indicator light that indicates ADSL layer connectivity. This indicator **MUST** function as follows:
- Solid Green = DSL good sync
 - Off = Modem power off
 - Flashing Green = DSL attempting sync
 - Flashing at 2 Hz with a 50% duty cycle when trying to detect carrier signal
 - Flashing at 4 Hz with a 50% duty cycle when the carrier has been detected and the modem is trying to train
- I - 32 The device **MUST** have an Internet indicator light that indicates whether or not it has at least one DSL device-controlled session up.
- This indicator **MUST** function as follows:
- Solid Green = IP connected (the device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has successfully complete – if used – and DSL is up) and no traffic detected.
 - If the IP or PPPoE session is dropped due to an idle timeout, the light will remain green if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.
 - Off = Modem power off, modem in bridged mode or ADSL connection not present
 - Flickering Green = IP connected and IP Traffic is passing thru the device (either direction)
 - Red = Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
- For bridged mode, the indicator light **MUST** be off.
- I - 33 The physical port indicator lamps **MUST** function as follows:
- Solid Green = Powered device connected to the associated port (includes devices with wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
 - Flashing Green = LAN activity present (traffic in either direction)
 - Off = No activity, modem power off, no cable or no powered device connected to the associated port.
- I - 34 The device **MUST** have a single function, recessed button with a red circle around it, in order to reset the device to the default factory settings.

- I - 35 The reset button on the device **MAY** be labeled as "reset" so a help desk can more easily identify it to a user.
- I - 36 Each port on the back of the device **MAY** have an icon displayed near it identifying the type of port.
- I - 37 The ports on the device **MUST** be identified by color with the appropriate connection/interface color reflected above, below or around each port.

The ports **MUST** be colored as follows:

- Ethernet Yellow
- Power Black
- Phone Grey
- USB Blue

The preferred Pantone colors for blue and yellow are:

- Blue 285C
- Yellow 114C
- Gray Cool Gray 3U (matte)

- I - 38 Each port on the back of the device **MUST** be labeled using icons and/or words, and any words must be spelled out completely (e.g., "Ethernet", "Power", ...).
- I - 39 The device **MUST** operate 24 hours a day, 7 days a week without the need to reboot.
- I - 40 The MTBF (Mean Time Between Failure) of the device and operating system **SHOULD** be equal to or exceed 1 year (e.g., it should not need a reboot more than one time per year).
- I - 41 The life expectancy of the device **SHOULD** be at least seven years.
- I - 42 The device **SHOULD** include sufficient non-volatile memory to accommodate future control and data plane protocol upgrades over a minimum of four years. The potential upgrades may include: initiating and terminating signaling protocols at IP and ATM layers; logic for packet classification, policing, forwarding, traffic shaping and QoS support at both IP and ATM layers.
- I - 43 The device **MUST** complete power up in 60 seconds or less (timing starts when the power is connected and stops when the On/Off power indicator light is "Solid Green").
- I - 44 The device **MUST** complete training within 60 seconds when autosensing is not activated (timing starts when the On/Off power indicator light is "Solid Green", when the DSLAM port is enabled and stops when the ADSL layer connectivity indicator is "Solid Green"). The default inner pair shall be used for this measurement.
- I - 45 The device **MUST** complete training within 60 seconds when autosensing is activated and ADSL is present on the default pair. The device **MUST** complete training within 120 seconds when autosensing is activated and ADSL is not present on the default pair.
- I - 46 [North America] The device **MUST** comply with FCC Part 15 rules for Class B devices.

- I - 47 [North America] The device **MUST** comply with Industry Canada ICES-003 Class B requirements.
- I - 48 [North America] The device **MUST** comply with Industry Canada's "Telecommunication Apparatus Compliance Specification" (IC document CS-03) and be registered with Industry Canada following the procedures highlighted in Industry Canada's "Procedure for Declaration of Conformity and Registration of Terminal Equipment" document (IC document DC-01).
- I - 49 [North America] The device **MUST** be certified to meet FCC Part 68, or obtain the appropriate waiver.
- I - 50 [North America] The device **MUST** comply with either:
 - TIA-968-A, Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network, October 2002,
 or both:
 - TIA/EIA/IS-968, Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment to the Telephone Network, July 2001, and
 - TIA/EIA/IS-883, Telecommunications - Telephone Terminal Equipment - Supplemental Technical Requirements for Connection of Stutter Dial Tone Detection Devices and ADSL modems to the Telephone Network, June 2001
- I - 51 [North America] The device **MUST** comply with the requirements of Telcordia™ GR-1089-CORE, Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment.
- I - 52 [North America] The device **MUST** support the following environmental conditions:

Environment	Temperature	Altitude	Relative Humidity	MWB
Operating (System Ambient)	0° C to 40° C	-197 to 7000 feet	8% to 95% non-condensing	23° C
Shipping and Storage	-25° C to 65° C		low humidity for low temperatures, 90% at 45° C, 30% at 65° C	29° C

- I - 53 This device **MUST** preserve local configuration information during power-off and power interruption.

2.2 WAN: ADSL and ATM

- I - 54 The device **MUST** include an internal ADSL modem.
- I - 55 The device **MUST** comply with requirements as specified in ANSI T1.413-1998, ANSI T1.413a-2001 and ITU 992.1.
- I - 56 The device **MUST** support FDM-mode per ANSI T1.413 and ITU-T G.992.1.

- I - 57 The device **SHOULD** comply with ITU G.992.3 (ADSL2) and ITU G.992.5 (ADSL2+) by 6/1/2004.
- I - 58 The device **SHOULD** comply with ITU G992.3 Annex L (RE-ADSL2) within three months after its approval.
- I - 59 The device **SHOULD** comply with ITU G992.5 Annex L (ADSL2) within three months after its approval.
- I - 60 The device **MUST** support Trellis coding.
- I - 61 The device **MUST** be rate-adaptive and able to support all speeds between the minimum and maximum applicable to the associated DSL protocol in use (e.g., ADSL, ADSL2, ADSL2+, RE-ADSL, ...) and in the minimum increment applicable to the associated DSL protocol in use.
- For example, for ADSL, the device **MUST** be able to support speeds in 32 kbps increments from 32 kbps to 8 Mbps downstream and 32 kbps to 800 kbps upstream.
- I - 62 The device **MUST** only synchronize within the minimum and maximum line rate parameters for a line as identified by the DSLAM or RT.
- I - 63 The device **MUST** support dynamic rate adaptation.
- I - 64 The device **MUST** support independent upstream and downstream data rate provisioning.
- I - 65 The device **MUST** support bit swapping.
- I - 66 The device **MUST** support both fast and interleaved paths. This is not a requirement for dual latency support (e.g., running Fast and Interleaved at the same time to two different locations).
- I - 67 The device **MUST** have a high-pass filter at its ADSL line input to eliminate impulse noise from premises wiring.
- I - 68 The device **SHOULD NOT** incorporate an internal splitter (i.e., **SHOULD NOT** have a POTS pass back port).
- I - 69 A failure in the device **MUST NOT** impact the private intra-premises network except for those functions provided by the device (i.e. DHCP, DNS, etc.).
- I - 70 The device **MUST NOT** cause any failure in or interference with the ADSL network.
- I - 71 The default pair used to detect the ADSL signal **MUST** be the inner pair (pins 3 & 4).
- I - 72 The device **SHOULD** automatically detect and select the ADSL signal on either the inner pair (pins 3 & 4) or outer pair (pins 2 & 5) of an RJ-11 jack
- If the modem reaches showtime after performing the DSL autosensing, the default pair will be set to the newly discovered pair. This can be the inner pair or the outer pair. The new default pair is store on the modem across power off situations. DSL autosensing will be activated with the new default pair.
- I - 73 If I - 72 is implemented, the device **MUST** allow disabling of the automatic detection of the ADSL signal on the inner and outer pairs and allow specification of which pair to search for the DSL signal.

- I - 74 Removing AC power from the device **MUST NOT** prohibit POTS from operating.
- I - 75 The CRC **MUST** conform to ANSI T1.413-1998 section 7.4.1.3.
- I - 76 The device performance and throughput **MUST** keep up with the DSL line rate.
- I - 77 Failure or removal of LAN CPE connected to the DSL device **MUST NOT** prohibit POTS from operating.
- I - 78 The device **MUST** support standard ATM (AAL5) payload format.
- I - 79 The device **MUST** perform AAL Segmentation and Reassembly (SAR), Convergence Sublayer (CS) functions and CRC check.
- I - 80 PCR shaping **MUST** be provided in the upstream direction when the interface between the PC and the device has more bandwidth than the ADSL connection provides.
- I - 81 The device **MUST** support ATM QoS. UBR, CBR and VBR-rt **MUST** be supported (as defined in The ATM Forum Traffic Management Specification Version 4.1).
- I - 82 VBR-nrt and UBR with per VC queuing **SHOULD** be supported.
- I - 83 The default ATM QoS for all VC's **MUST** be UBR.
- I - 84 The device **MUST** support multiple levels of QoS listed above simultaneously across separate VCCs (e.g., UBR for PVC 0/35 and CBR for PVC 0/43 where both PVCs are active simultaneously).
- I - 85 The device **SHOULD** support auto configuration as defined in DSL Forum TR-037 and ILM1 4.0 and its extensions.
- I - 86 The device **MUST** always respond to ATM testing, pings and loopbacks according to ITU-T I.610 (F4, F5).
- I - 87 The device **MUST** support 0/35 as the default VPI/VCI for the first PVC.
- I - 88 The device **MUST** be able to perform an auto search for the VPI/VCI settings for the first PVC. This search **MUST** be the following VPI/VCI's in sequence looking for a first-success: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59.
 The default VPI/VCI identified in I - 87 is searched prior to this auto search list.
 If the modem reaches a state of session establishment (e.g., IP when the modem is responsible for session termination) after performing the auto search, the default VPI/VCI settings will be set to the newly discovered values. The new default pair is stored on the modem across power off situations. If an ATM connection cannot be established after a power restoral, the search process starts over again.
- I - 89 The device **MUST** be configurable so that the auto-search mechanism can be disabled.
- I - 90 The device **MUST** allow the auto-search list to be redefined using the XML based interface.
- I - 91 The default VPI/VCI values for all PVCs **MUST** be configurable. The default value **MUST** be utilized prior to performing an auto-search but should exclude the default value in the auto-search.
- I - 92 The device **MUST** support VPI values from 0 to 255

- I - 93 The device **MUST** support VCI values from 32 to 65535
- I - 94 The device **MUST** pass the tests identified in DSL Forum TR-048, "ADSL Interoperability Test Plan", and any subsequent updates or replacements to that document that exist at the time that the modem is tested, prior to its initial deployment.
Within 6 months, modems produced after changed or new test requirements have been approved **MUST** conform to those new requirements.
- I - 95 The device **MUST** train and pass data against all ITU 992.1 based ATU-C deployed in North America using TR-048 (and future updates).

2.3 Multiple PVCs

- I - 96 The device **MUST** support eight PVCs.
- I - 97 There is no default defined VPI/VCI past the first PVC which is identified in I - 87 above. Auto-search is supported on all PVCs and will use the same auto-search sequence identified (skipping over any already in use). This auto-search is defined in I - 88 through I - 90.
- I - 98 All supported PVCs **MUST NOT** require the same VPI value.
- I - 99 All supported PVCs **MUST** be able to be active and sending/receiving traffic simultaneously. See I - 119, I - 120, I - 210 and I - 211 for more details on interface selection for routing.
- I - 100 The device **MUST** support the minimum ATM granularity applicable to the associated DSL protocol in use on a per VC and VP basis.
For example, ATM granularity of 32 kbps **MUST** be supported for ADSL on a per VC and VP basis.

2.4 WAN: Access Protocols

- I - 101 The device **MUST** be a learning bridge as defined in IEEE 802.1D for all logical and physical Ethernet interfaces, supporting a minimum of 272 MAC addresses.
- I - 102 The device **MUST** support Ethernet (IEEE 802.3).
- I - 103 The device **MUST** support encapsulation of bridged Ethernet over AAL5 (without FCS) as described in IETF RFC 2684 (formerly IETF RFC 1483).
- I - 104 The device **MUST** be able to use both LLC-SNAP and VC-MUX (null) encapsulation over AAL5 with all supported protocols. The default **MUST** be LLC-SNAP.

- I - 105 The device **MUST** support the TCP, IP, UDP, routing and associated protocols identified here:
- IETF RFC 0768 User Datagram Protocol
 - IETF RFC 0791 Internet Protocol
 - IETF RFC 0792 Internet Control Message Protocol
 - IETF RFC 0793 Transmission Control Protocol
 - IETF RFC 0826 Ethernet Address Resolution Protocol (ARP)
 - IETF RFC 0894 Standards for the Transmission of IP Datagrams over Ethernet Networks
 - IETF RFC 0922 Broadcasting Internet Datagrams in the Presence of Subnets
 - IETF RFC 0950 Internet Standard Subnetting Procedure
 - IETF RFC 1009 Requirements for Internet Gateways (Link Layer issues only)
 - IETF RFC 1042 Standard for the Transmission of IP Datagrams over IEEE 802 Networks
 - IETF RFC 1112 Host Extensions for IP Multicasting
 - IETF RFC 1122 Requirements for Internet Hosts - Communication Layers
 - IETF RFC 1123 Requirements for Internet Hosts - Application and Support
 - IETF RFC 1256 ICMP Router Discovery Messages (Router Specification only)
 - IETF RFC 1519 Classless Inter- Domain Routing (CIDR)
 - IETF RFC 1812 Requirements for IP Version 4 Routers
 - IETF RFC 1918 Address Allocation for Private Internets
 - IETF RFC 3600 Internet Official Protocol Standards
 - IANA Directory of General Assigned Numbers (<http://www.iana.org/numbers.html>)
- I - 106 The device **MUST** support IP over the encapsulated Ethernet.
- I - 107 The device **MUST** be able to bridge IP over Ethernet.
- I - 108 The device **MUST** be able to route IP over Ethernet to LAN CPE.
- I - 109 The device **MAY** support encapsulation of IP over AAL5, per IETF RFC 2684.
- I - 110 If the device supports IP over AAL5, it **MAY** support Classical IP according to IETF RFC 2225.
- I - 111 The device **MUST** include built-in PPPoE client functionality.
- I - 112 [TR-059] The device **MUST** be capable of initiating at least two PPPoE sessions per PVC and route the IP traffic above that to the LAN CPE.
- I - 113 The device **MUST** allow the protocol stack (e.g., IP over Ethernet, PPPoE, PPPoA, etc...) for each provisioned PVC to be defined separately. If necessary, each PVC can use a different stack and set of protocols.
- I - 114 The device **MUST** support PPPoE over the encapsulated Ethernet as defined in IETF RFC 2516.

- I - 115 The device **MUST** support mini-jumbo frames when bridging Ethernet over AAL5 such that it will be possible to allow establishment of PPPoE protocols from the device with ultimate 1500 byte Ethernet or IP payloads.

For example, in the PPPoE case the WAN side encapsulations would be:

WAN (ATM CPCS-PDU payload)

	Ethernet Header (bytes)	PPPoE header (bytes)	PPP protocol id (bytes)	IP Data (bytes)	Total Bytes
1500 Byte Ethernet (with LLC/SNAP)	26	6	2	38 - 1492	72 - 1526
1500 Byte IP (over Ethernet with LLC/SNAP)	26	6	2	38 - 1500	72 - 1534

- I - 116 The device **MUST** support manually setting, through the GUI and XML interfaces, an MTU to be used in negotiating MTU, overriding the default MTU.

- I - 117 The device **MUST** support PPP and the associated protocols identified below:

- IETF RFC 1332 The PPP Internet Protocol Control Protocol (IPCP)
- IETF RFC 1334 PPP Authentication Protocols (PAP)
- IETF RFC 1661 The Point-to-Point Protocol (PPP)
- IETF RFC 1877 PPP IPCP Extensions for Name Server Addresses (limited to DNS addresses unless the device supports NetBIOS)
- IETF RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)

- I - 118 The device **MUST** support the following:

- IETF RFC 1570 PPP LCP Extensions
- IETF RFC 2153 PPP Vendor Extensions

This is not stating that specific extensions **MUST** be supported. It is identifying that upon receipt of non-standard or unrecognized PPP extensions from the DSL network (e.g., vendor or proprietary), the device **MUST** operate without fault.

- I - 119 [TR-059] The device **MUST** allow for the selection of which traffic to forward over which connection (in the case of multiple PVCs, multiple PPPoE sessions, etc...) according to any one or more of the following pieces of information:
- (1) destination IP address(es) with subnet mask,
 - (2) originating IP address(es) with subnet mask,
 - (3) source MAC address,
 - (4) destination MAC address,
 - (5) protocol (TCP, UDP, ICMP, ...)
 - (6) source port,
 - (7) destination port,
 - (8) IEEE 802.1D user priority,
 - (9) FQDN (Fully Qualified Domain Name) of WAN session,
 - (10) DiffServ codepoint (IETF RFC 3260),
 - (11) Ethertype (IEEE 802.3, 1998 Length/Type Field), and
 - (12) traffic handled by an ALG.
- I - 120 [TR-059] The device **SHOULD** allow for the selection of which traffic to forward over which connection (in the case of multiple PVCs, multiple PPPoE sessions, etc...) according to any one or more of the following pieces of information:
- (1) IEEE 802.1Q VLAN identification, and
 - (2) packet length.
- I - 121 [TR-059] The device **MUST** be able to bridge or route IP over an Ethernet session concurrently with at least one device-originated PPPoE session on each PVC that is running bridged Ethernet over the AAL.
- I - 122 The device **MUST NOT** bridge or route between WAN connections (i.e., WAN to WAN) except when explicitly configured to do so.
- I - 123 The device **SHOULD** support PPPoA as defined in IETF RFC 2364.
- I - 124 The device **MUST** be configured by default to PPPoE.
- I - 125 PPPoE bridging and associated operation in the device **MUST NOT** fail nor operate improperly in the presence of vendor-specific PPPoE extensions which may be in use by LAN devices (i.e., the device **MUST** interoperate with well known PPPoE client software).
- I - 126 The device **MUST** be able to save all logins and passwords for PPP sessions originated by the device. Passwords **MUST NOT** be available outside of the internal operation of the device (e.g., can not be queried nor displayed).

- I - 127 The device **MUST** support an "always on" mode for connections. In this mode the device **MUST NOT** time out DSL sessions (ATM, IP and PPP) and **MUST** automatically re-establish any sessions after disconnection, lease expiration or loss and restoration of power.
- I - 128 The device **MUST** support a "connect on demand" option for connections. In this mode the connection to the DSL network is initiated when outbound traffic is encountered from the local LAN and terminated after a timeout period in which no traffic occurs.
- I - 129 The device **MUST** support a "manual connect" option for connections. In this mode the connection to the DSL network is initiated manually through the GUI or an XML request and, by default, terminates only when done so explicitly by the user, due to a power loss or when the connection is lost.
- I - 130 The default mode for connections **MUST** be "connect on demand".
- I - 131 The interval after which a connection timeout occurs **MUST** be able to be configured.
- I - 132 A manual way of disconnecting without waiting for a connection timeout **MUST** be provided.
- I - 133 A default timeout of 20 minutes **SHOULD** be used for connection timeouts.
- I - 134 The device **MUST** not immediately terminate PPPoE sessions and upper layer protocol connections when the physical connection is lost. It should defer the tear down process for two minutes. If the physical connection is restored during that time, the device **MUST** first attempt to use its previous PPPoE session settings. If these are rejected, then the original PPPoE session can be terminated and a new PPPoE session attempted.
- I - 135 The device **SHOULD** incorporate a random timing delay prior to starting each IP and PPP session.
- This random timing delay helps to reduce connection failures when a group of users attempt to establish connections to a service provider at the same time (e.g., after restoral of power to a neighborhood that had a blackout).
- I - 136 The device **SHOULD** not attempt immediate additional PPP session connections upon receipt of an authentication failure. A back off mechanism **SHOULD** be implemented to limit repeated attempts to reconnect in this situation. 3 connection attempts **SHOULD** be made followed by a delay and then repeated by the next sequence of connection attempts. The delay **SHOULD** be 5 minutes at first, and then repeated every 30 minutes as required.
- This requirement only applies to automated connection attempts.
- I - 137 The device **MUST** be able to bridge PPPoE sessions initiated from LAN devices (sometimes known as PPPoE pass-through).
- Only PPPoE traffic **MUST** be bridged unless bridging of other traffic is specifically enabled.
- I - 138 The device **MUST** support a minimum of eight LAN device initiated PPPoE sessions from each LAN device.
- I - 139 The device **MUST** be able to bridge eight sessions per PVC.

- I - 140 The device **MUST** be able to bridge PPPoE sessions at all times when encapsulating Ethernet over AAL5. This applies when the device has set up zero or more PPPoE sessions and/or when the device is also running IP over Ethernet. The default setting **MUST** be for this pass-through to be on.
- I - 141 The device **MUST** allow for pass-through of IP traffic in which the payload is compressed or encrypted (e.g., VPN traffic). This means other LAN CPE **MUST** be able to originate PPTP and L2TP sessions to an external network (over IP).
- I - 142 The device **MUST** allow LAN CPE to originate IPsec sessions to an external network. This function **MUST** work properly through the NATP function of the DSL device.
- I - 143 The device **MUST** allow at least one IPsec connection from the LAN.
- I - 144 The device **SHOULD** allow multiple users on the LAN to launch independent and simultaneous IPsec sessions.
- I - 145 The device **MUST** support LAN device UDP Encapsulation of IPsec packets as defined in draft-ietf-ipsec-udp-encaps-08.txt and its successors.
- I - 146 The device **MUST** support LAN device negotiation of NAT-Traversal with IKE as identified in draft-ietf-ipsec-nat-t-ike-08.txt and its successors.
- I - 147 A minimum of 4 concurrent LAN IPsec sessions **SHOULD** be supported per LAN device. These sessions can be to the same or unique destinations.
- I - 148 The device **MUST** support Path MTU discovery (described in IETF RFC 1191) so that a LAN device can be told what to set its MTU to.

2.5 LAN: Physical Interfaces

- I - 149 The device **MUST** support use of a straight-through (patch) cable between the Ethernet Interface and a PC.
- I - 150 The device **SHOULD** automatically sense the transmit and receive pair on the Ethernet physical connection.
- I - 151 The device **MUST** have at least one 10BASET Ethernet port (RJ-45 jack) for connecting it to the home data network.
- I - 152 If the device supports 100BASET it **MUST** be able to support both 10BASET and 100BASET with auto negotiate for speed and duplex on a port-by-port basis according to IEEE 802.3u.
- I - 153 The device **MUST** support, at a minimum, a 256 MAC address table for LAN devices.
- I - 154 The Ethernet LAN interface **SHOULD** allow for adjusting the inter-frame and collision back off timers so that P traffic (as defined in IEEE 802.1P) can get statistically better treatment on broadcast LAN Segments.
- I - 155 The device **SHOULD** have a client USB port (series "B" receptacle), allowing it to be a non-powered (i.e., it has its own power source and doesn't get power across the USB interface) slave device for a host computer.

- I - 156 If the device has a client USB port, the USB interface **MUST** appear to the PC or other host device to be an Ethernet port (i.e., the PC drivers are Ethernet drivers), and not appear as a DSL modem (i.e., **MUST NOT** require DSL modem drivers on LAN CPE).
- I - 157 If the device has a client USB port, the USB port **MUST** be based on the USB 1.1 (or later) technical specification.
- I - 158 If the device has a client USB port and USB 2.0 is supported, the USB interface **MUST** still work with the USB 1.1 based USB host controller based on the USB 2.0 standard.
- I - 159 Over the USB interface, the device **SHOULD** support USB drivers for Windows 98, Windows 98 Second Edition, Windows Millennium Edition, Windows XP (Home and Professional), Windows 2000, Macintosh OS 8.6, Macintosh OS 9.x and Macintosh OS 10.x. Any drivers that are PC-based or run on the PC **SHOULD** be Microsoft WHQL certified. Drivers **SHOULD** be available for new Microsoft and Macintosh operating systems within 30 days of General Availability.
- I - 160 The USB port **MUST** be covered with a sticker than warns the customer not to install the USB cable until instructed to do so in the documentation or installation software.
- I - 161 If the device has only one Ethernet port and only one client USB port, the device **SHOULD** be configurable through XML so that only the Ethernet or client USB port is to be active at any one time. In this configuration, whenever one of the ports is in use, the other is disabled. If neither is in use, both are enabled. The default configuration of the device **SHOULD** be that both ports are active at the same time.

2.6 WAN and LAN: IP Addressing and DHCP Server

- I - 162 [TR-059] The device **MUST** support classification of WAN directed LAN traffic and placement into appropriate queues based on any one or more of the following pieces of information:
 - (1) destination IP address(es) with subnet mask,
 - (2) originating IP address(es) with subnet mask,
 - (3) source MAC address,
 - (4) destination MAC address,
 - (5) protocol (TCP, UDP, ICMP, ...)
 - (6) source port,
 - (7) destination port,
 - (8) IEEE 802.1D user priority,
 - (9) FQDN (Fully Qualified Domain Name) of WAN session,
 - (10) Diffserv codepoint (IETF RFC 3260),
 - (11) Ethertype (IEEE 802.3, 1998 Length/Type Field), and
 - (12) traffic handled by an ALG.

- I - 163 [TR-059] The device **SHOULD** support classification of WAN directed LAN traffic and placement into appropriate queues based on any one or more of the following pieces of information:
- (1) IEEE 802.1Q VLAN identification, and
 - (2) packet length.
- I - 164 [TR-059] The device **MUST** support the differentiated services field (DS Field) in IP headers as defined in IETF RFC 2474.
- I - 165 [TR-059] The device **MUST** be able to mark or remark the Diffserv codepoint or IEEE 802.1D user priority of traffic based on the classification information identified in I - 162 and I - 163 above.
- I - 166 [TR-059] The device **MUST** support one Best Effort (BE) queue, one Expedited Forwarding (EF) queue and a minimum of four Assured Forwarding (AF) queues.
- I - 167 [TR-059] The device **MUST** duplicate the set of queues for each access session. This can be done logically or physically.
- I - 168 [TR-059] The device **SHOULD** support the appropriate mechanism to effectively implement Diffserv per hop scheduling behaviors. A strict priority scheduler is preferred for EF.
- I - 169 [TR-059] The device **MUST** support the capability to fragment AF and BE traffic in order to constrain the perturbing impact of AF and BE packets on EF traffic delay, for example using a mechanism such as MLPPP LFI [IETF RFC1990].
- I - 170 [TR-059] The packet size threshold before fragmenting AF and BE packets **MUST** be configurable.
- I - 171 The device **MUST** be able to obtain IP network information dynamically on its WAN interface. This information includes IP address, primary and secondary DNS addresses and default gateway address.
- Dynamically obtaining IP network information is accomplished using DHCP and / or IPCP.
- I - 172 If PPP is used, the device **MAY** obtain an IP subnet mask on its WAN interface using IPCP extensions. If this is done, then IP subnet masks will be communicated with IPCP using the PPP IPCP option with option code 144, the length of the option being 6 and the mask being expressed as a 32-bit mask (e.g. 0xFFFFFFFF80), not as a number indicating the consecutive number of 1s in the mask (from 0 to 32).
- The learned network information **MAY**, but need not, be used to populate the LAN side embedded DHCP server for the modem.
- The learned network information is treated as a subnet and not as a collection of individual addresses. That is, the first and last address in the subnet should not be used.
- The IP address negotiated should, but need not, be the one assigned to the modem.
- I - 173 If the device is not configured to use a static IP address and the modem fails to detect a PPPoE or DHCP server, then the WAN IP address assignment value **SHOULD** be set to an undefined value, in order to prevent it from retaining its prior IP address.

- I - 174 The device **MUST** provide application layer support for host name mapping, booting, and management including DHCP and the Domain Name System (DNS) protocol. This includes support for the standards below:
- IETF RFC 1034 Domain Names - Concepts and Facilities
 - IETF RFC 1035 Domain Names - Implementation and Specification
 - IETF RFC 2131 Dynamic Host Configuration Protocol
 - IETF RFC 2132 DHCP Options and BOOTP Vendor Extensions
 - IETF RFC 2181 Clarifications to the DNS Specification
 - IETF RFC 2939 Procedure for Defining New DHCP Options and Message Types
- I - 175 The device **MUST** be a DHCP server to local LAN devices, supporting all LAN devices.
- I - 176 The embedded DHCP server function of the device **MUST** be able to operate while in bridged mode. The default state should be on in bridged and router mode.
- I - 177 The device **MUST** support a minimum of 253 LAN devices.
- I - 178 The device **MUST** support turning off the embedded DHCP server via a configuration change.
- I - 179 The device **MAY** incorporate auto-detection of other DHCP servers on the local LAN and, if configured to do so, disable the internal DHCP server functionality of the DSL device in this situation.
- In this situation, the DSL device would try to obtain a configuration for its LAN port through DHCP. If a DHCP response was received, the device would then use the information in the DHCP response (e.g., IP Address, subnet and DNS information) and disable its internal DHCP server. If implemented and a DHCP response is received, this requirement takes precedence over I - 190.
- I - 180 The embedded DHCP server functionality of the device **MUST** verify that an address is not in use prior to making it available in a lease (e.g., via Ping or ARP table validation) even when lease information shows that it is not in use.
- I - 181 The device **MUST** support all LAN devices concurrently accessing one or more WAN connections.
- I - 182 The device **MUST** use the default start address of 192.168.1.64 and the default stop address of 192.168.1.253 for assignment to DHCP leases for local device addressing.
- I - 183 The device **MUST** use a default netmask of 255.255.255.0 for assignment to DHCP leases for local device addressing.
- I - 184 The device **MUST** be able to be configured to specify alternate public and private subnets (without restriction) for local device addressing.
- I - 185 The device **MUST** be able to be configured to specify the start and stop addresses within a subnet used for local addressing.
- I - 186 The default lease time for DHCP information provided to LAN CPE which do not share the WAN side IP address **MUST** be configurable. The default value **MUST** be 24 hours.

- I - 187 The default lease time for DHCP information provided to LAN CPE which share the WAN side IP address **MUST** be configurable. The default value **MUST** be 10 minutes.
- I - 188 When the domain name that the embedded DHCP server passes to LAN CPE has not been set, the value "domain_not_set.invalid" **SHOULD** be used.
- I - 189 When the device's embedded DHCP server is enabled, the device itself **MUST** default to the address 192.168.1.254 (with a netmask of 255.255.255.0).
- I - 190 When the device's embedded DHCP server is disabled, the device **MUST** ARP for the following addresses, in order, and assign itself the first one that is not taken: 192.168.1.254, 192.168.1.63, and then starting from 192.168.1.253 and descending.
- I - 191 The device **MUST NOT** use auto IP for address assignment of its LAN-side address.
- I - 192 The device **MUST** allow its assigned address and netmask to be specified through the XML and GUI interfaces.
- I - 193 The device **MAY** support SOCKS (IETF RFC 1928) for non-ALG access to the public address.
- I - 194 Both NetBios and Zero Config naming mechanisms **MAY** be used to populate the DNS tables.
- I - 195 The device **MAY** act as a NETBIOS master browser for that name service.
- I - 196 The device **MUST** support multiple subnets being used on the local LAN.
- I - 197 The device **MUST** be able to assign its WAN IP address (e.g., public address) to a particular LAN device, concurrent with private IP addressing being used for other LAN CPE.

In this situation, one device on the LAN is given the same public IP address (through DHCP or manual configuration of the LAN CPE IP stack). Other LAN devices utilize private IP addresses. The device can then be configured as identified in I - 219 so that the LAN device "sharing" the WAN IP address receives all unidentified or unsolicited port traffic to any specific LAN device. If the device is not configured in this manner, then only inbound traffic resulting from outbound traffic from the LAN CPE would be directed to that LAN CPE.

The gateway identified to the LAN device must be on the same subnet as that associated with the WAN IP address. Note that the use of the WAN gateway address does not guarantee this since it need not meet this requirement.

- I - 198 When using a WAN IP address assigned to a LAN device, the user **MUST** be able to configure if this LAN device can directly communicate with other CPE on the local LAN.

This will only be done to the extent which the device can control the isolation (e.g., routing and internal switch fabric). It does not extend to isolation external to the device (e.g., external switch or router) which are outside of the control of the device.

- I - 199 The device **MAY** allow the embedded DHCP server to be configured so that specific MAC addresses can be identified as being served or not served.

- I - 200 The device **MAY** allow the embedded DHCP server to be configured with a default setting (provide IP addresses or do not provide IP addresses) for devices with unspecified MAC addresses.
- I - 201 The embedded DHCP server functionality of the device **SHOULD** provide a mechanism by which an IP address can be assigned to a particular LAN device by MAC address. The user interface to establish this association may use an alternate mechanism to identify this assignment (e.g., by selecting the device using its current IP address or device name) and the MAC address may be transparent to the user. These addresses may include the ability to assign an address outside of the default subnet, as identified in I - 184 and I - 197.

For example, the device might have a default WAN side IP address which is used for NAT to a subset of devices and an additional set of WAN side IP addresses which are bridged. The embedded DHCP server might be used to assign this second set of IP addresses to specific LAN CPE.

- I - 202 The device **MUST** support a single PC mode of operation. In this mode of operation only a single LAN device is supported. Note that this is not the default mode of operation.

In this configured mode, all network traffic, except for configured management traffic destined for the modem itself (e.g., temporary remote access to the GUI) **MUST** be passed between the DSL network and the designated LAN device as if the DSL device was not present.

One possible implementation is for the embedded DHCP server to issue one and only one private address in this situation, with the start and stop address for the embedded DHCP server being the same.

The LAN device can be assigned either a private IP address (i.e., using 1:1 NAT) or the public IP address (i.e., using IP Passthrough) of the modem (as identified in I - 197). The type of IP address to be used (private or public) is configured through the GUI and XML interfaces. The default is a public IP address.

If a WAN connection is not available when the device is configured to use a public IP address, the LAN device is provided with a private IP address from the device via DHCP. Once a WAN connection is established, the public IP address provided by the DSL network is passed to the LAN device during the next DHCP lease renewal.

The DSL device acts as the default gateway to the LAN devices when private IP addressing is in use. When public IP addressing is in use, the gateway identified to the LAN device should be that identified in I - 197 above.

No other restrictions (e.g., restricted routing for other devices) need to be implemented to meet this requirement (e.g., no routing restrictions on traffic from secondary devices on the LAN).

- I - 203 The device **MUST** operate by default in the multiple PC mode of operation (i.e., full NAT router).
- I - 204 The device **MUST** support IP Version 4.

- I - 205 The device **SHOULD** be software configurable or upgradeable to support IP Version 6 in the future.

This means that the processing power, memory and networking components must be designed appropriately and be sufficiently robust to provide this support.

2.7 Routing and NAPT

- I - 206 The device **MUST** support Network Address Port Translation (NAPT; also known as Port Address Translation) as identified in the documents below:
- a) IETF RFC 2663 IP Network Address Translator Terminology and Considerations
 - b) IETF RFC 3022 Traditional IP Network Address Translator
 - c) IETF RFC 3027 Protocol Complications with the IP Network Address Translator

- I - 207 The device **MUST** support disabling NAPT.

- I - 208 The device **MUST** maintain route table entries for all connections it maintains on the WAN (e.g., per PVC, IP and PPP sessions) and for all LAN networks (including subnets).

- I - 209 The device **SHOULD** be able to restrict the routing information for each WAN connection to specific LAN devices.

For example, a user might have four PCs in their home, have a WAN connection to the Internet and have a WAN connection to an employer's network. The device could be configured to allow all PCs access to the Internet, but only one specific PC might be allowed to send traffic over the WAN interface to the employer's network.

- I - 210 [TR-059] The device **MUST** support the ability to accept IP routes dynamically pushed from the WAN. This allows it to set up routing tables to support routing traffic over multiple connections (PVCs, PPPoE sessions, etc...). In particular, the device **MUST** be configurable to accept RIP Version 2 (RIP-2, IETF RFC 2453) messages to fulfill this task.
- I - 211 [TR-059] The device **MAY** support additional mechanisms to accept IP routing information.
- I - 212 [TR-059] RIP-2 functionality **SHOULD** be software configurable.
- I - 213 By default, the device **MUST NOT** transmit RIP-2 information to WAN connections.
- I - 214 The device **MUST** include port forwarding configurations and Application Level Gateways (ALGs) for the following applications and protocols that do not function properly with NAT or NAPT: FTP client, H.323, SIP, IPSec, PPTP, MSN Messenger, AOL Instant Messenger, Yahoo Messenger and ICQ.
- I - 215 The device **SHOULD** include port forwarding configurations and ALGs for other major applications and protocols that do not function properly with NAT or NAPT. Some potential candidates are identified in Appendix A.
- I - 216 The ALG mechanism **MUST** be integrated with the port forwarding mechanism.

- I - 217 The device **MUST** support port forwarding. That is, the device **MUST** be able to be configured to direct traffic based on any combination of source IP address, source protocol (TCP and UDP) and port (or port range) to a particular LAN device and port (or port range on that device).

Individual port forwarding rules **MUST** be associated with a LAN device, not the IP address of the LAN device, and follow the LAN device should its IP address change.

- I - 218 The port forwarding mechanism of the device **SHOULD** be easy to configure for common applications and user protocols (e.g., ftp, http, etc.) by specifying a protocol name or application instead of a port number and protocol type. A partial list of applications for potential inclusion are identified in Appendix A.

- I - 219 The port forwarding mechanism **MUST** be able to be configured to direct all unidentified or unsolicited port traffic to any specific LAN device.

The LAN device may be using either a private IP address or the public WAN IP address (as identified in I - 197).

2.8 Firewall

- I - 220 The device **MUST** provide Denial of Service (DOS) protection for itself and all LAN CPE including protection from Ping of Death, SYN Flood LAND and variant attacks.

The extent of this protection will be limited when the device is configured as a bridge in which only PPPoE traffic is bridged. This protection **MUST** be available when the device terminates IP or bridges IP.

- I - 221 The device **MUST** reject packets from the WAN with MAC addresses of devices on the local LAN or invalid IP addresses (e.g., broadcast addresses, private IP addresses or IP Addresses matching those assigned to the LAN Segment).

- I - 222 The device **MUST** drop or deny access requests from WAN side connections to LAN side devices and the DSL device itself except in direct response to outgoing traffic or as explicitly permitted through configuration of the DSL device (e.g., for port forwarding or management).

- I - 223 The device **MAY** support a more robust firewall, such as one which provides a full OSI 7 layer stack stateful packet inspection and packet filtering function.

- I - 224 The device **MAY** support a separate firewall log to maintain records of all transactions that violate firewall rules.

- I - 225 The firewall log file **SHOULD** be able to hold at least the last 100 entries or 10 Kbytes of text.

- I - 226 If a firewall log is implemented, the file entries **SHOULD** not be cleared, except when the device is reset to its factory default settings.

- I - 227 If a firewall log is implemented, the device **MUST** timestamp each firewall log entry.

2.9 Naming Services

- I - 228 The device **MUST** act as a DNS name server to LAN devices, passing its address back to these devices in DHCP requests as the DNS name server.
- I - 229 The device **SHOULD** allow the user to specify that the network learned or user specified DNS addresses be passed back to the LAN devices in DHCP responses instead of the DSL modem address itself as the DNS name server(s).
- I - 230 When the device learns DNS name server addresses from multiple WAN connections, the DSL device **MUST** query a server on each connection simultaneously and provide the requesting LAN client with the first returned positive result from these DNS servers. A negative response will not be transmitted to a LAN device until all WAN DNS servers have either timed out or returned a negative response to a common query.

Service providers may choose not to provide DNS name server addresses on certain connections in a multiple connection configuration.
- I - 231 The device **MUST** add the DNS entry "dsldevice" for its own address.
- I - 232 The device **MAY** support additional DNS entries, as there could be additional types of CPE.
- I - 233 The device **MUST** maintain local DNS entries for a minimum of 253 local LAN devices. This information can be obtained through auto discovery (e.g., from DHCP requests, such as Client Identifier, and other protocol information). When unknown, the entry **MUST** be of the form "unknownxxxxxxxxxxxx" where "x" represents the MAC address of the associated LAN device.
- I - 234 The device **SHOULD** provide a manual mechanism for overriding the learned names of all LAN CPE except that for the DSL device itself.

2.10 User Interface and Management

- I - 235 A console port that allows end user access (e.g., placed on the outside of the device) **SHOULD NOT** be provided on the device.
- I - 236 The device **SHOULD** be self-installable by an end user in under 20 minutes assuming the default configuration and mode of operation for the device. This is the time from when the box is opened to the user is surfing including any driver installation (assuming no network complications and excluding micro-filter installation and customer ordering/registration).
- I - 237 Configuration and installation of the device **SHOULD** minimize the number of restarts of the device when enabling changes.
- I - 238 If software is loaded on LAN CPE for installation or configuration of the device, this software **MUST NOT** require the associated LAN CPE to restart, except in the case of the installation of networking drivers (e.g., USB, wireless, etc...) or a change in the IP address assignment (e.g., static to DHCP, public to private, private to public or assignment of a specific IP address using DHCP).

- I - 239 Other than networking drivers (e.g., USB, wireless, etc...), other software or drivers **MUST NOT** be required for proper and full use of the device.
- I - 240 If UPnP IGD is supported, it **MUST** be disabled as a default.
- I - 241 If UPnP IGD is supported, the user **SHOULD** be warned upon enabling it that this may allow applications to configure the box and allow unexpected traffic to access local devices.
- I - 242 If UPnP IGD is supported, it **MUST** allow the user to log all UPnP IGD actions and events.
- I - 243 An XML based WAN side auto configuration mechanism **MUST** be supported as defined in DSL Forum TR-069.
- I - 244 A configuration mechanism from the PC to the device based on XML **MUST** be supported as defined in DSL Forum Working Text TR-064.
- I - 245 The XML based LAN side configuration mechanism **MUST** operate independently of the status or configuration of UPnP IGD in the device.
- I - 246 The device **MUST** be configurable via embedded, easy-to-use web pages.
- I - 247 XML and GUI authorization **MUST** time out after 30 minutes.
- I - 248 The web pages **MUST** be available when the device is in bridged mode.
- I - 249 The device, drivers and any packaged software **SHOULD** support Macintosh OS 8.6 and above.
- I - 250 The device, drivers and any packaged software **SHOULD** support all Microsoft PC based operating systems which have not yet reached "End of Life" status (see <http://www.microsoft.com/windows/lifecycleconsumer.mspx> for more details).
- I - 251 The device, drivers and any packaged software **MAY** support Linux. It is especially desirable to do so with an open interface.
- I - 252 The device **MUST NOT** require browser support of Java, ActiveX nor VBSCRIPT in its web pages.
- I - 253 The web pages **SHOULD** minimize internal page complexity (e.g., excessive use of frames, pop-ups, style sheets, JavaScript, etc...) that places demands on browser resources or causes interoperability problems with different browsers. In general, all pages **SHOULD** load within five seconds.
- I - 254 The web interface **MUST** be OS independent and browser independent (e.g., must work with Opera, Mozilla, Safari, Netscape and Internet Explorer).
The web interface **MUST** work with Netscape 4.7, Microsoft Internet Explorer 4.0 and later versions of these browsers.
- I - 255 The device **MUST** have a software mechanism by which the user can reset it to default factory settings.
- I - 256 The device **MUST** support a modem access code (i.e., password) that protects it from being updated (firmware, configuration, operational state, etc...) from the local LAN. Additional password discussion is identified in DSL Forum TR-064 and TR-069.

- I - 257 The device modem access code **MUST** be set to a default modem access code of a length of 10 decimal digits (0 through 9).
- I - 258 The default modem access code **SHOULD** be unique for each DSL device, when in factory default mode or pre-installation mode (e.g., as shipped or after a modem reset to factory defaults).
- I - 259 The device modem access code **MUST NOT** be displayed nor broadcast in any way by the device (e.g., through HTML or as a MAC address).
- I - 260 The default modem access code **MUST** be on the bottom of the DSL device.
- I - 261 The device **MUST** force the user to accept the default modem access code or install a new modem access code prior to allowing any initial configuration (e.g., during initial installation or after a modem reset to factory defaults).
- I - 262 The user **MUST** be able to disable the use of the modem access code. The user **MUST** be warned in the GUI of the implications of under-taking this action.
- I - 263 The device **MUST** be able to provide web pages to allow temporary manual remote access to its GUI from the WAN. Primary requirements relating to this mode of operation are identified in I - 264 through I - 275 below.
- I - 264 When temporary WAN side remote access is enabled to the device, the remote access session **MUST** be started within 20 minutes and the activated session **MUST** time out after 20 minutes of inactivity.
- I - 265 The user **MUST** be able to specify that the temporary WAN side remote access is a read only connection or one which allows for updates. The default **MUST** be read only.
- I - 266 Temporary WAN side remote access **MUST NOT** allow for changing the device password.
- I - 267 Temporary WAN side remote access **MUST** be disabled by default.
- I - 268 Temporary WAN side remote access **SHOULD** be through HTTP over TLS (i.e., https using TLS).
- I - 269 The device **SHOULD** use a randomly selected port for temporary WAN side remote access to prevent hacking of a well known port.
- I - 270 If a default port is used for temporary WAN side remote access, it **MUST** be 51003.
- I - 271 The user **MUST** specify a non-blank password to be used for each temporary WAN side remote access session. This information **MUST** not be saved across sessions.
- I - 272 The User ID for all temporary WAN side remote access sessions, if required based on the method of implementation, **MUST** be "tech" by default.
- I - 273 The user **MUST** be able to change the User ID for all temporary WAN side remote access sessions.
- I - 274 The device **MUST** allow only one temporary WAN side remote access session to be active at a time.
- I - 275 All other direct access to the device from the WAN side **MUST** be disabled and blocked by default.

- I - 276 The device **MUST** support updating of its firmware via the GUI and XML interfaces.
- I - 277 The device **MUST** use standard protocols when using FTP and HTTP (e.g., FTP - IETF RFC 959, HTTP - IETF RFC 2616, HTTPS - IETF RFCs 2246, 2818).
- I - 278 The vendor **SHOULD** have a web site where firmware updates and documentation is available.
- I - 279 The documentation **SHOULD** include manuals containing detailed installation procedures, corrective actions for troubleshooting, and subsequent release notes for all software versions, network driver versions, modem firmware versions, fixes and changes.
- I - 280 The firmware at the vendor's web site **SHOULD** include all error correcting updates for the device.
- I - 281 All software revisions **SHOULD** be backward compatible with all previous versions. There **SHOULD** be no loss of existing functionality.
- I - 282 Software revisions **MUST NOT** require service provider network changes to maintain proper operation of previous features.
- I - 283 The vendor of the device **MUST** adhere to a vendor self-defined standard numbering and revisioning scheme for all firmware releases and all documentation.
- I - 284 The device **MUST NOT** allow "back door" entry to the unit (e.g., there must be no hidden telnet or web access using secret passwords).
- I - 285 All firmware updates **MUST** be verified using security mechanisms. A checksum mechanism is a minimum requirement for achieving this.
- I - 286 All firmware updates **SHOULD** be verified using an acryptographic "fingerprint" of at least 256 bits.
- I - 287 In the event of a failure occurring during an update, the device **SHOULD** be able to back off to the prior version of the firmware installed on the DSL device.

That is, the prior version of the device's firmware **SHOULD** continue to be useable in the event that a firmware update fails to complete.

This is not a requirement for a dual image, but that is one manner in which this requirement might be achieved.
- I - 288 The device **MUST** have diagnostics tools that allow the user to identify the precise nature of any connection or performance problem. It **MUST** be able to indicate if the problem is at the ADSL, ATM, Ethernet, PPP, or IP layer. These tools **MUST** be accessible from the GUI and XML interfaces.
- I - 289 The device **MUST** provide detailed information for current connections and associated parameters including ADSL sync rate, power for both upstream and downstream directions, FEC error count, CRC error count, line attenuation, signal-to-noise margins, relative capacity of line, trained bit rate, graph of bits per tone, and loss of signal, loss of frame and loss of power counts. Additional parameters are identified in TR-064 and TR-069.

- I - 290 The device **MUST** support restarting the broadband connection (all layers) via the GUI and XML interfaces.
- I - 291 The device **MUST** follow all standards required to perform an orderly tear down of the associated connections involved at the associated network levels (e.g., issue a DHCPRELEASE message when using DHCP, issue LCP Terminate-Request/Terminate-Ack and PADT packet when using PPPoE, etc.) and then restart the connections.
- I - 292 The model and serial number **MUST** be visible via external markings on the device.
- I - 293 The device **MUST** support remote testing, remote diagnostics, performance monitoring, surveillance information access and other information access as identified in ANSI T1.413-1998 and ITU G.997.1. At a minimum non-optional requirements from these standards **MUST** be supported. Additional parameters are identified in TR-064, TR-069, I - 288 and I - 289.
- I - 294 The device **MUST** maintain an internal log of ATM status and WAN side connection flows (e.g., DHCP, IP and PPP sessions). At a minimum, the log **MUST** record the last 250 modem events. This will include modem training events initiated by the modem or by the DSLAM. The purpose of the log is to provide a trouble shooting aid in resolving line and connection problems.
- I - 295 The device **MUST** timestamp each log entry.
- I - 296 The factory default timestamp value for log entries **SHOULD** indicate the elapsed time since the unit was first powered on. The log entry timestamp **SHOULD** be formatted, consistent with ISO 8601:2000, as follows:

PYYYY-MM-DDThh:mm:ss

where:

- P = the letter "P" used to indicate what follows is a time interval (period) data element
- YYYY = number of years (digits)
- MM = number of months (digits, 01 – 12; 1 month is the equivalent of 30 days for time interval purposes)
- DD = number of days (digits, 01 – 30)
- hh = number of hours (digits, 00 – 24)
- mm = number of minutes (digits, 00 – 60)
- ss = number of seconds (digits, 00 – 60)

Once the device has established connectivity to an Internet based time server, all log entry timestamps **SHOULD** be formatted for GMT or user specified time zone (24 hour military format), consistent with ISO 8601:2000, as follows:

YYYY-MM-DDThh:mm:ss±hh:mm or

YYYY-MM-DDThh:mm:ssZ ,

where:

YYYY = year (digits)

MM = month (digits, 01 – 12)

DD = day of month (digits, 01 – 31)

T = the letter “T”, used to indicate the start of the time of day

Z = the letter “Z”, used to indicate that the time is UTC (Coordinated Universal Time)

hh = hours (digits, 00 – 24)

mm = minutes (digits, 00 – 60)

ss = seconds (digits, 00 – 60)

±hh:mm = the difference between local time and UTC in hours and minutes (e.g., -05:00 would indicate Eastern Standard Time, 5 hours behind UTC)

- I - 297 The device **SHOULD** be able to copy log files to a PC on the local LAN or network server in ASCII text format, using the GUI and XML interface.
- I - 298 The device modem log **SHOULD** reside on the device and be persistent across power loss.
- I - 299 The device modem log **SHOULD NOT** interfere with the normal performance of the modem. That is, the prioritization of writing log entries to non-volatile storage **SHOULD NOT** be done at a priority or in a manner that would degrade the user experience nor the connection throughput.
- I - 300 The device **MUST** support an internal clock with a date and time mechanism.
- I - 301 The device clock **MUST** be able to be set via an internal time client using NTP (IETF RFC 1305) or SNTP (IETF RFC 2030) from an Internet source.
- I - 302 The device **MUST** support the use of time server identification by both domain name and IP address.
- I - 303 If the device includes default time server values, they **SHOULD** be specified by domain name and not by IP address.
- I - 304 The device **SHOULD** allow configuration of the primary and alternate time server values in addition to or in place of any default values.

- I - 305 If the device includes default time server values or time server values are identified in documentation, these values **SHOULD** be selected using industry best practices.
- For example, draft-mills-sntp-v4-00.txt identifies that the time server names used should be those of servers the manufacturer or seller operates as a customer convenience or those for which specific permission has been obtained from the operator of the time server.
- I - 306 The time client **SHOULD** re-resolve any time server IP address obtained from a domain name on a periodic interval, but not less than the time-to-live field in the DNS response.
- I - 307 The time client **SHOULD** support DNS responses with CNAMEs or multiple A records.
- I - 308 The default frequency with which the device updates its time from a time server **MUST NOT** be less than 60 minutes.
- I - 309 The default frequency with which the device updates its time from a time server **MUST NOT** be greater than 24 hours.
- I - 310 The frequency with which the device updates its time from a time server **SHOULD** be able to be configured.
- I - 311 The time server discovery and selection stage used by the time client **SHOULD** check each candidate time server in a round robin fashion, with a response timeout between each request to each time server.
- If no time server has responded during a round of checking, the response timeout **SHOULD** be exponentially incremented (e.g., doubled) and the time servers checked again.
- The round robin checking and exponential incrementing of the response timeout **SHOULD** continue until a time server is discovered or a search limit is reached.
- I - 312 The device **SHOULD** support the [S]NTP access-refusal mechanism, so that a server returning a Stratum value of zero (0; sometimes termed a kiss-o'-death reply) in response to a client request causes the client to cease sending requests to that server.
- If this occurs during the discovery and selection stage for a time server, then the discovery mechanism should continue on to the next time server in its list of those to check or increase the response timeout as identified above.
- If this occurs when the device is periodically updating its clock, then the discovery and selection stage for a time server should be re-initiated.
- I - 313 The device **SHOULD** validate response packets for malformed time protocol packets (invalid flags – such as client query flag, bad packet size, ...) and ignore invalid packets.
- I - 314 The device **SHOULD** ignore time protocol response packets with a source IP address other than that of the time server that the modem queried.

- I - 315 The device **MUST** be able to start training, establish a network connection and respond to network tests by default upon power up prior to any additional configuration or software installation on the associated PC. The absence of a PC **MUST** have no impact on these operations.
- I - 316 The device **MUST** make the access concentrator name used with PPPoE connections available via XML and GUI for diagnostic purposes.
- I - 317 The device **MUST** have a PING client built into the unit.
- I - 318 The device **MUST** detect the loss of communications with a network identified DNS server as indicated by a failed query, and upon failed query, log the event.

2.11 Graphical User Interface

2.11.1 General

- I - 319 The device **MUST** have a quick start page allowing for rapid configuration in a minimum number of steps (e.g., on a single page). Default values for PPPoE and PVC can be used to facilitate this.
- I - 320 The model and firmware/software versions **MUST** be easily identifiable via the GUI interface.

2.11.2 Software Updates

- I - 321 The web interface **MUST** allow the user to browse and select an update file from a local PC and use HTTP to update the device using this file (see IETF RFCs 1867, 2388 and HTML 4.1 specifications for more details).
- I - 322 If the device has been configured to do so, the web interface **MUST** allow the user to specify that firmware be updated from a pre-defined web location. The device **MUST** allow the web location to be specified by either WAN side or LAN side mechanisms as identified in I - 243 and I - 244.
- I - 323 The web location **MAY** be pre-defined by the modem manufacturer. This value is overridden by the mechanisms and information identified in I - 322.
- I - 324 If the device has been configured to allow updating from a pre-defined web location, the device **MUST** display an update button in the GUI. The user can then select the update button to initiate an update using a file retrieved via ftp or http as identified in the associated URL (2 URLs may be hard coded; the second URL will be used if file retrieval is not possible from the first URL).
- I - 325 If the device has been configured to allow updating from a pre-defined web location, the mechanism used to identify the availability of an update, the description of the update and the actual update **SHOULD** operate solely based on the presence (or absence) of named files returned in a directory list using the web location URL.

For example, a device might retrieve the directory list, find the update associated with the modem by the presence of the following file:

Vendor-model-v100210-n100215.pkg

This would identify that for device "model" from "vendor" currently running version 10.02.10 there exists an update whose version is 10.02.15. The text describing the update, if available, might be located in a file of the name:

Vendor-model-v100210-n100215.txt

- I - 326 If the device has been configured to do so, the web interface **MUST** display a web link to which the user may go to browse for update files and other update information. The device **MUST** allow this URL to be specified by either WAN side or LAN side mechanisms as identified in I - 243 and I - 244.
- I - 327 The web link **MAY** be pre-defined by the modem manufacturer. This value is overridden by the mechanisms and information identified in I - 326.
- I - 328 The device **MUST** preserve its configuration across firmware updates.

2.12 Packaging

- I - 329 Cables **MUST** be colored as identified in I - 37.
- I - 330 The device **MUST** be packaged with a quick start or installation guide.
- I - 331 The Quick Start Guide **SHOULD** be made available in alternate formats including large print.
- I - 332 All necessary end user documentation **MUST** be included with the device.
- I - 333 Additional detailed product documentation **SHOULD** be included with the device.
- I - 334 The model and serial number **MUST** be visible via external markings on the product packaging.
- I - 335 All device firmware and associated system files **MUST** be pre-installed.
- I - 336 A phone cable with two pairs and RJ-11 endpoints **MUST** be packaged with the product to connect the device to the ADSL wall jack on the WAN interface. The cable **MUST** be a minimum length of 6 feet. The endpoints **MUST** meet the specifications for a miniature 6-position plug in TIA-968-A.
- I - 337 The phone cable **SHOULD** be CAT3 or CAT5 and be a length of 14 feet.
- I - 338 A CAT5 (or better) straight through (patch) Ethernet cable with RJ-45 endpoints **MUST** be packaged with the product to connect the device to the first computer. The cable **MUST** be a minimum length of 6 feet. The endpoints **MUST** meet the specifications for a miniature 8-position unkeyed plug in TIA-968-A.
- I - 339 If the device has a USB port, the packaging **MUST** clearly state for which operating systems this is supported.
- I - 340 If the device has a client USB port, a USB Implementers Forum certified USB 2.0 high-speed cable **MUST** be packaged with the device. The cable **MUST** be a minimum length of 6 feet.

APPENDIX A Application Level Gateway (ALG) and Port Forwarding List

This appendix is a partial list of applications and protocols which should work through the usage of pre-defined port forwarding configurations and ALGs. It is not a comprehensive list of all applications. It is not a comprehensive list of all applications. It is expected that support for more applications will be needed with time.

A

Active Worlds, Age of Empires, Age of Kings, Age of Wonders, Aliens vs. Predator, America Online, Anarchy Online, AOL Instant Messenger, Asheron's Call, Audiogalaxy Satellite

B

Baldur's Gate, BattleCom, Battlefield communicator, Black and White, Buddy Phone

C

Calista IP Phone, Camerades, CarbonCopy32 host, Citrix Metaframe / ICA Client, Counter Strike, CU-SeeMe

D

Dark Reign, Dark Reign 2, Decent 3, Decent Freespace, Deerfield MDAemon EMail Server, Delta Force, Delta Force 2, Delta Force: Land Warrior, Delta Three PC to Phone, Descent 3, Descent Freespace, Diablo (1.07+), Diablo I, Diablo II (Blizzard Battle.net), Dialpad, Direct Connect, DirectX Games, DNS Server, Doom, Doom Server, Drakan, Dwyco Video Conferencing

E

Elite Force, Everquest

F

F-16, Mig 29, F-22, Lightning 3, F-22 Raptor, F-22 Raptor (Novalogic), Falcon 4.0, Fighter Ace II, Figher Ace II for DX play, FlightSim98, FreeTel, FTP Client, FTP Server, FW1VPN

G

GameSpy Online, Ghost Recon, GNUtella, Go2Call

H

H.323, Half Life, Half Life Server, Heretic II Server, Hexen II, HomeWorld, Hotline Client, Hotline Server, HTTP Server, HTTPS Server

I

I'76, ICMP Echo, ICQ Old, ICQ 2001b, ICUII Client, ICUII Client Version 4.xx, iGames, IMAP Client, IMAP Client v.3, IMAP server, Internet Phone, Internet Phone Addressing Server, iPhone, IPsec Encryption, IPsec ESP, IPsec IKE, IRC, IStreamVideo2HP, Ivisit

K

Kali, Doom & Doom II, KaZaA, Kojan Immortal Sovereigns

L

L2TP, LapLink Gold, LapLink HOSt, Limewire, LIVvE, Lotus Notes Server

M

MechWarrior 3, Medal of Honor: Allied Assault, Microsoft DirectPlay, Midtown Madness, mIRC DCC, IRC DCC, mIRC Chat, mIRC IDENT, Monopoly Host, Motocross Madness, Motorhead Server, MPlayer Games Network, MSN Game Zone, MSN Game Zone (DX 7 & 8 play), MSN Messenger, Myth (Bungie.net, Myth II)

N

Napster, Need for Speed 3, Hot Pursuit, Need for Speed 5, Porsche, Net2Phone, NetMech, NetMeeting, Default PC, NNTP Server, Nox, ntald Traditional Unix Talk Daemon, NTP

O

OKWeb, OKWin, Operation FlashPoint, Outlaws

P

Pal Talk, pcAnywhere v7.5, pcAnywhere host, pcAnywhere remote, PCTelecommute, Phone Free, POP Client, POP3 Server, Polycom ViaVideo H.323, PPTP

Q

Quake 2, Quake 3, Quake 3 Server, QuickTime Server, QuickTime/Real Audio Client, QuakeWord,

R

Rainbow Six, RAdmin, RDP, RealAudio, Red Alert, Remote Anything, Remote Desktop 32, Remotely AnyWhere, Remotely Possible Server, Return to Castle Wolfenstein, Rise of Rome, Rlogin/Rcp, Roger Wilco, Rogue Spear, RTSP

S

Scour Media, SDP, Shiva VPN, Shout Cast Server, SIP, SMTP Server, Soldier of Fortune, Speak Freely, SQL*NET Tools, SSH Secure Shell, SSH Server, StarCraft, Starfleet Command, Starsiege: Tribes, SWAT3

T

Telnet Server, The 4th Coming, Tiberian Sun: Command & Conquer III (& Dune 2000), Timbuktu Pro, Total Annihilation

U

Ultima Online, Unreal Server, Unreal Tournament, USENET News Service

V

VNC, Virtual Network Computing, VDO Video, VoxChat, VoxPhone 3.0

W

Warbirds 2, Webcam (TrueTech), Webcam32, Webforce Compcore MPEG-1 Player2.0, Web Server, WebPhone 3.0, Westwood Online, C&C, Windows 2000 Terminal Server

Base Requirements for an ADSL Modem with Routing

X

X Windows, XP Remote Desktop

Y

Yahoo Messenger Chat, Yahoo Pager, Yahoo Messenger Phone

Z

ZNES

APPENDIX B Example Queuing for a DSL Router

Figure 1 shows the queuing and scheduling discipline envisioned for upstream traffic through the DSL router in support of future services offerings delivered over the architecture described in TR-059.

There are multiple access sessions supported in this model, however, all traffic is classified and scheduled in a monolithic system. So, while it might appear at first that the Diffserv queuing and scheduling might apply only to IP-aware access – in fact all access, IP, Ethernet, or PPP is managed by the same system that adheres to the Diffserv model.

For example, at the bottom of the figure, BE (Best Effort) treatment is given to the non-IP-aware access sessions (PPPoE started behind the DSL Router or delivered to an L2TP tunnel delivery model). This queue might be repeated several times in order to support fairness among multiple PPPoE accesses – or it may be a monolithic queue with separate rate limiters applied to the various access sessions.

The PTA access is a single block of queues. This is done because NSP access typically works with a single default route to the NSP, and managing more than one simultaneously at the RG would be perilous. The Σ rate limiter would limit the overall access traffic for a service provider.

Rate limiters are also shown within the EF and AF service classes because the definition of those Diffserv types is based on treating the traffic differently when it falls into various rates.

Finally, at the top of the diagram is the ASP access block of queues. In phase 1A of the TR-059 architecture, these queues are provisioned and provide aggregate treatment of traffic mapped to them. In phase 1B, it will become possible to assign AF queues to applications to give them specific treatment instead of aggregate treatment. The EF service class may also require a high degree of coordination among the applications that make use of it so that its maximum value is not exceeded.

Notable in this architecture is that all the outputs of the EF, AF, and BE queues are sent to a scheduler (S) that pulls traffic from them in a strict priority fashion. In this configuration EF traffic is, obviously, given highest precedence and BE is given the lowest. The AF service classes fall in-between.

Note that there is significant interest in being able to provide a service arrangement that would allow general Internet access to have priority over other (bulk rate) services.¹ Such an arrangement would be accomplished by assigning the bulk rate service class to BE and by assigning the default service class (Internet access) as AF with little or no committed information rate.

¹ This “bulk rate” service class would typically be used for background downloads and potentially for peer-to-peer applications as an alternative to blocking them entirely.

Given this arrangement, the precedence of traffic shown in the figure is arranged as:

1. EF – red dotted line
2. AF – blue dashed line (with various precedence among AF classes as described in IETF RFC 2597)
3. BE – black solid line

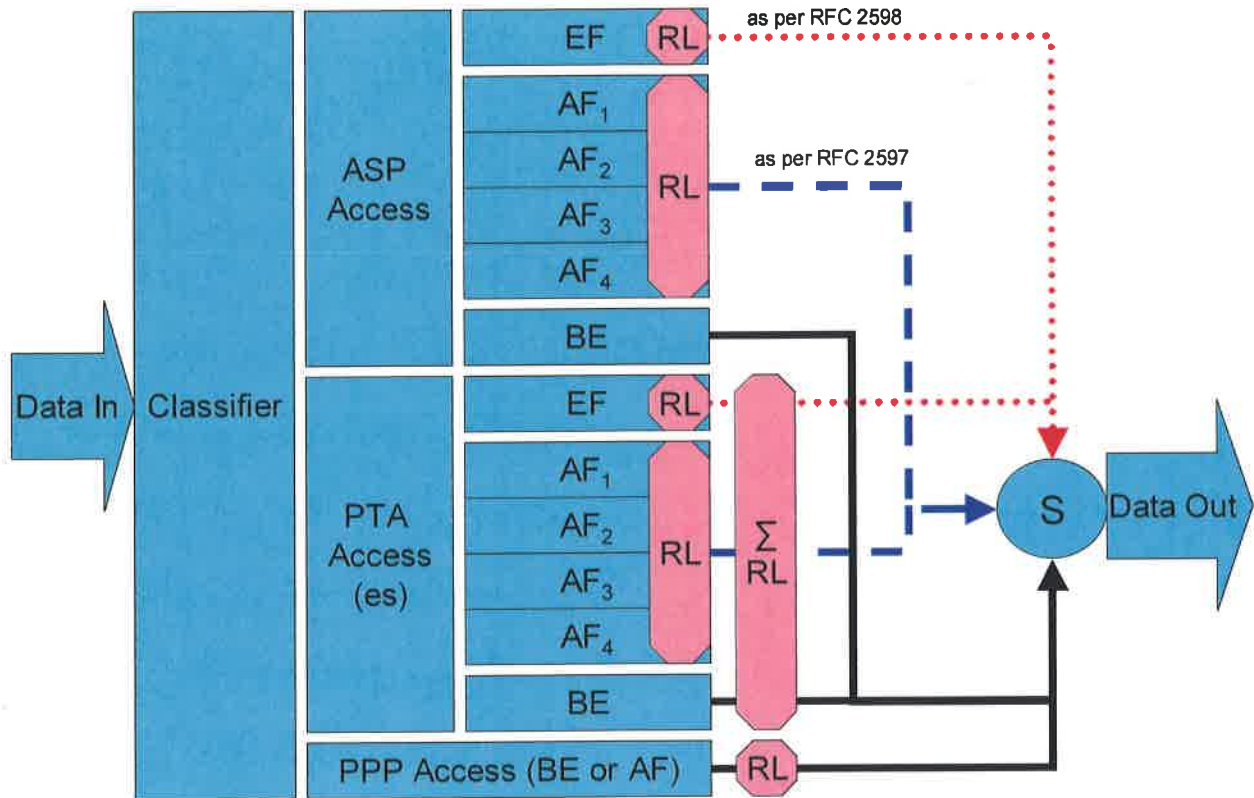


Figure 1 - Queuing and Scheduling Example for DSL Router

In Figure 1 the following abbreviations apply:

- ASP – Application Service Provider
- PTA – PPP Terminated Aggregation
- PPP – Point-to-Point Protocol
- EF – Expedited Forwarding – as defined in IETF RFC 3246
- AF – Assured Forwarding – as defined in IETF RFC 2597
- BE – Best Effort forwarding
- RL – Rate Limiter
- ΣRL – Summing Rate Limiter (limits multiple flows)
- S – Scheduler

APPENDIX C Examples of Potential Configurations

C.1 Introduction

The pictures and descriptions in the following scenarios are intended to provide examples of the interworking of many of the requirements in this document.

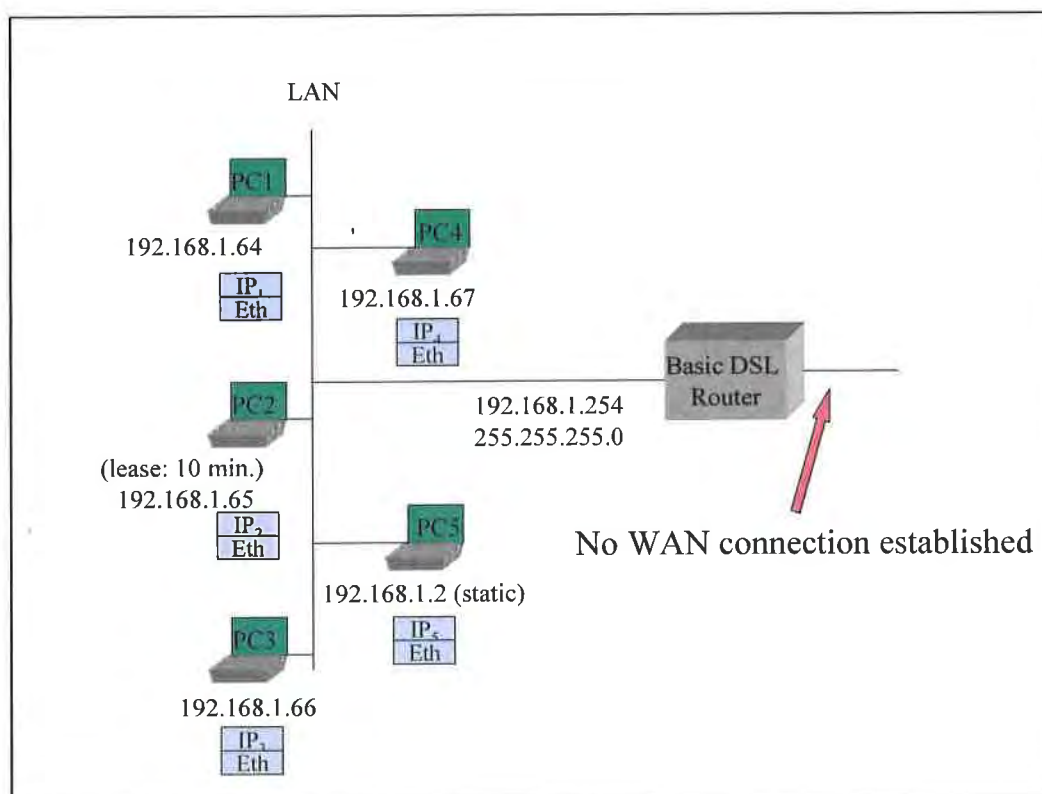
Since the single PC case is a simple subset of the multi-PC case (except when explicitly using the single PC mode of operation [I - 202], see the scenario in Section C.5), it will not be directly addressed. The network that will be used in this sequence of examples has 5 PCs. They are described as being connected over Ethernet. Naturally, there could easily be wireless, powerline, or phoneline networking used. The actual physical medium is not relevant. The PCs could also be devices other than PCs. That is also not relevant to these scenarios.

C.2 Basic DSL Modem as Router Initiating One or More PPPoE Sessions

The four scenarios that follow build upon one another to describe a number of the capabilities required in this document. They show PPPoE being used in all cases for WAN connectivity, with the embedded DHCP server in the DSL router enabled.

C.2.1 No WAN Connection

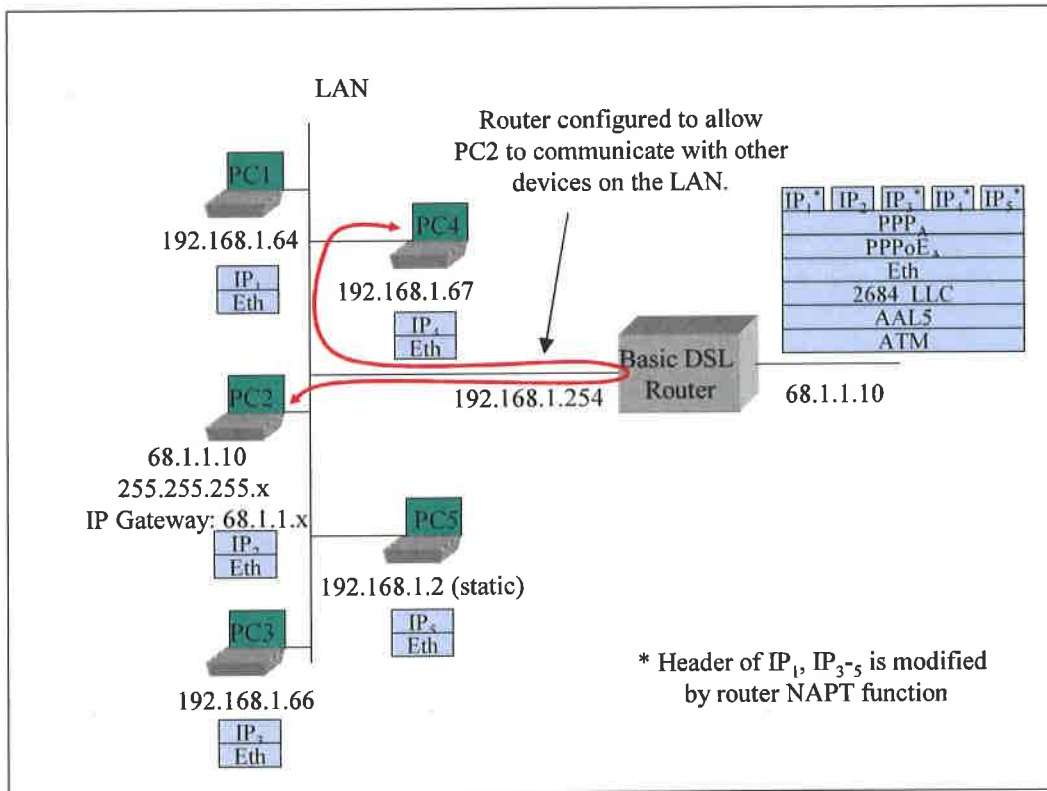
- The router has no WAN connection up.
- The router has been configured to give PC2 its WAN address via its embedded DHCP server. Since the router has no WAN connection, it will give PC2 a private address with a 10 minute lease time [I - 187].
- PC5 has been configured with a static IP address.
- PCs 1-4 are configured to make DHCP requests. The router responds to all DHCP requests with IP addresses in the range of 192.168.1.64 to 192.168.1.253 [I - 182], an IP gateway address (and LAN-side address of the device) of 192.168.1.254 [I - 189], a DNS server address of 192.168.1.254 [I - 228] and an IP address lease time for all PCs but PC2 of 24 hours [I - 186].



C.2.2 Router Sets Up PPPoE to an ISP

This scenario is the same as presented above with the following exceptions:

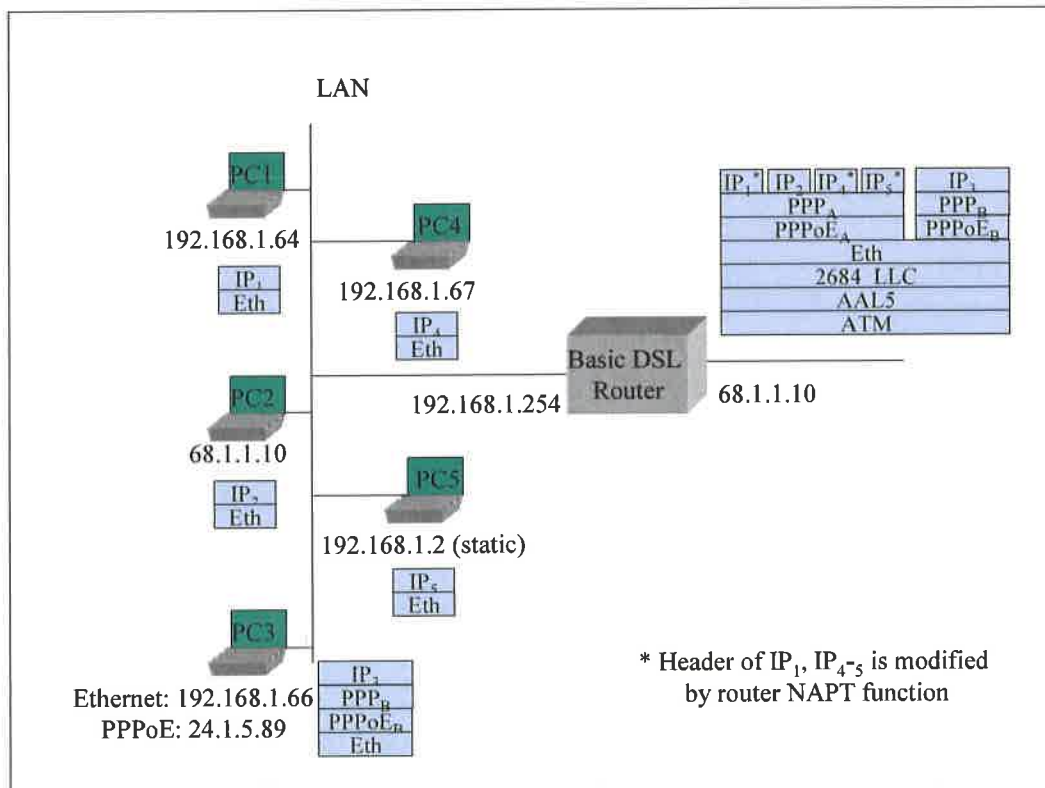
- The router sets up a PPPoE session to ISP – it obtains an IP address and DNS server addresses via IPCP [I - 103, I - 104, I - 111, I - 117, I - 171].
- The router gives its public IP address to PC2 [I - 197].
- The router is configured to allow PC2 to communicate with other devices on the LAN [I - 198].



C.2.3 PC3 Sets Up Its Own PPPoE Session

This scenario is the same as presented above with the following exceptions:

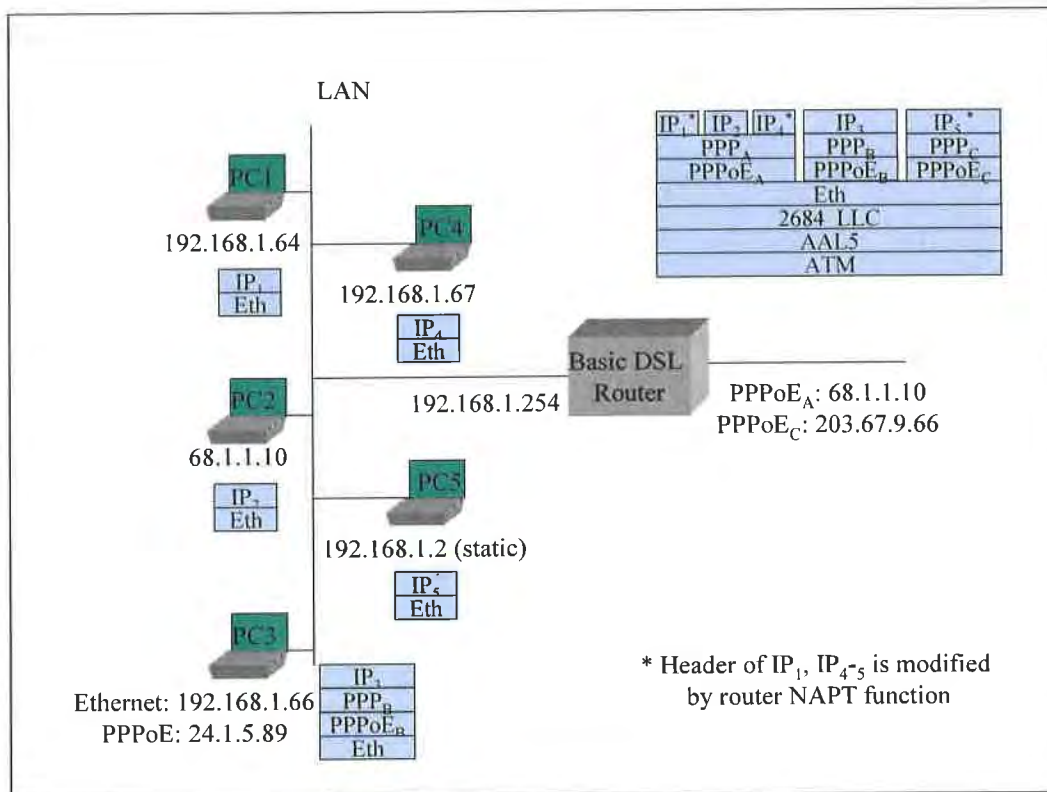
- PC3 uses a PPPoE client to establish its own PPPoE session. While the private IP address from the router is still associated with PC3's Ethernet interface, PC3 also has a public IP address associated with its own PPPoE interface. Common behavior is for all IP traffic of PC3 to now use this PPPoE interface [I - 137, I - 140].



C.2.4 Router Sets Up a Second PPPoE Session

This scenario is the same as presented above with the following exceptions:

- The router sets up second PPPoE session (PPPoE_C). It gets an IP address and DNS addresses through IPCP. It gets routing information from RIP-2 [I - 210], manual entry, or other mechanisms [I - 211]. PPPoE_A remains the default route [I - 112].
- PC5 requests a DNS lookup for a URL. The router sends simultaneous URL lookup requests to DNS servers on both PPPoE connections. The DNS server on the PPPoE_A connection fails to resolve the URL and the PPPoE_C connection returns an IP address. The router returns the IP address to PC5 [I - 230].
- PC5 sends IP packets to the returned IP address. The router determines from its routing table that this goes to the PPPoE_C connection.

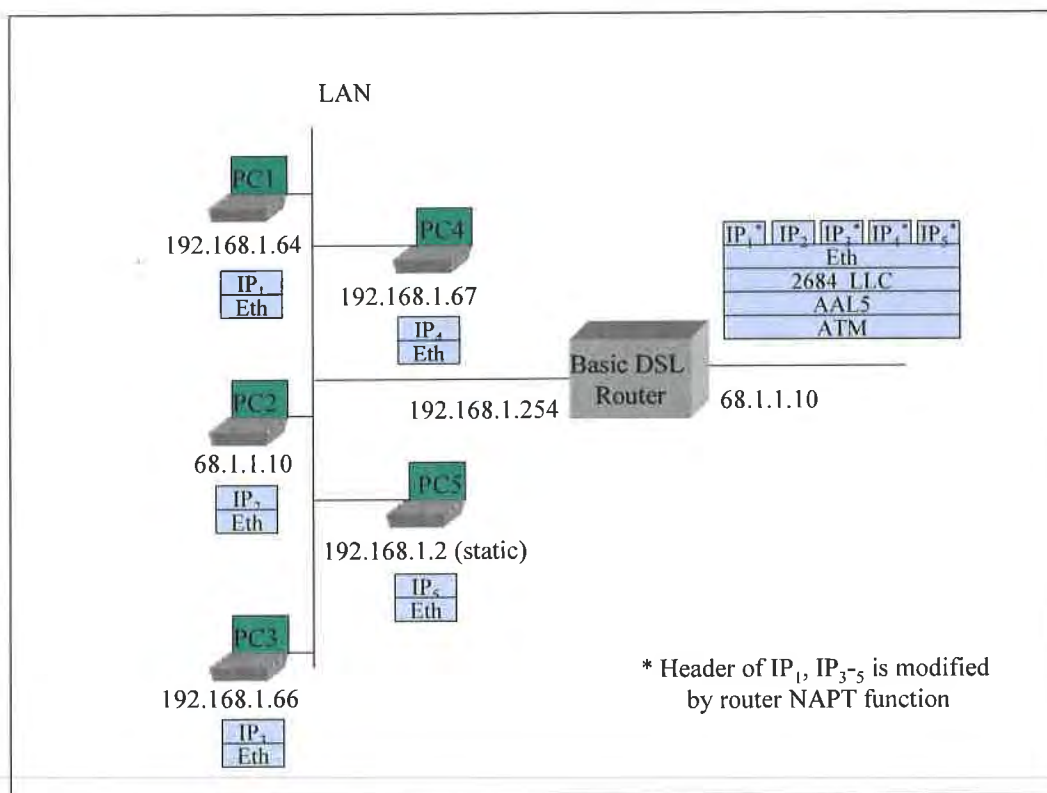


C.3 “2684 Bridged” Mode

The next three scenarios deal with cases where either the network is not expecting any PPP login or the router is not doing any PPP. The first case has the router using its DHCP client to the WAN, acting as a DHCP server to the LAN, and doing routing and NAT to PCs on the LAN. The second case has the router not establishing a WAN connection, and individual PCs setting up their own PPPoE sessions. In the third case, the router’s embedded DHCP server is also disabled, and the PCs are getting IP addresses from the WAN.

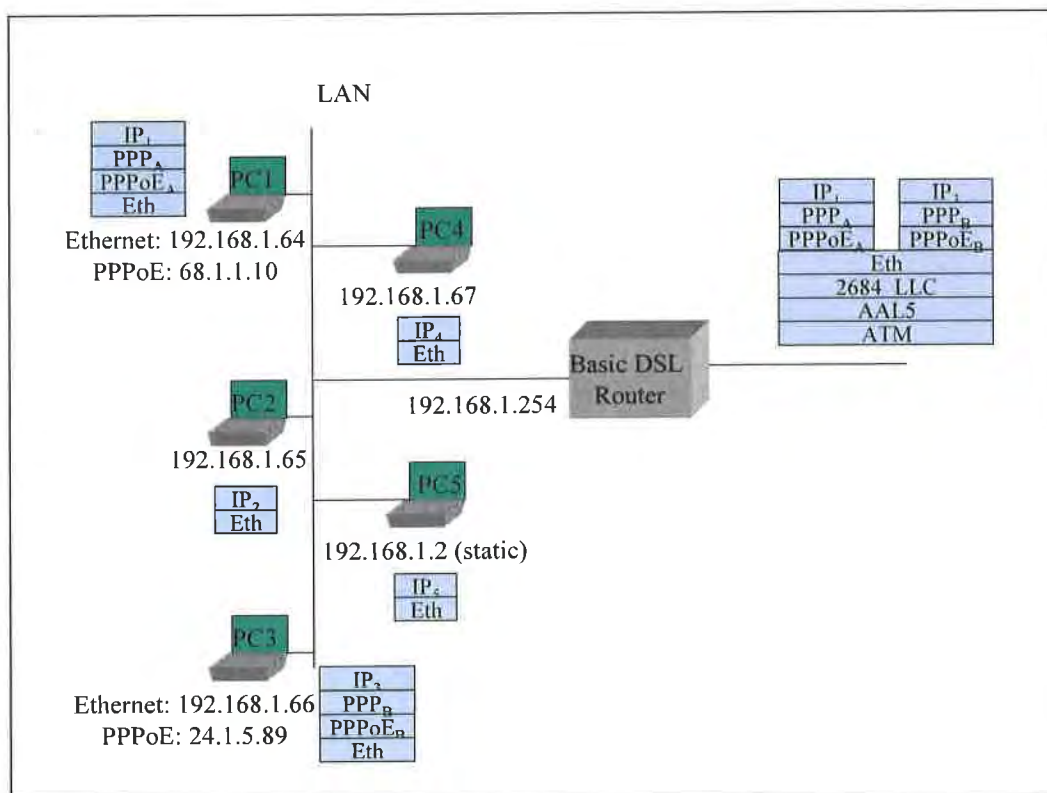
C.3.1 Router in IP-routed “2684 Bridged” Mode, Embedded DHCP Server On

- The router provides an IP address to each device that it receives a DHCP request from.
- PC5 uses a static IP address and does not send a DHCP request to the router.
- The router has been configured to give PC2 its WAN address. When the router has no WAN connection, it gives PC2 a private address with a short lease time.
- The router issues a DHCP request and establishes an IP session to the WAN [I - 103, I - 104, I - 108].
- The router gives its public IP address to PC2.



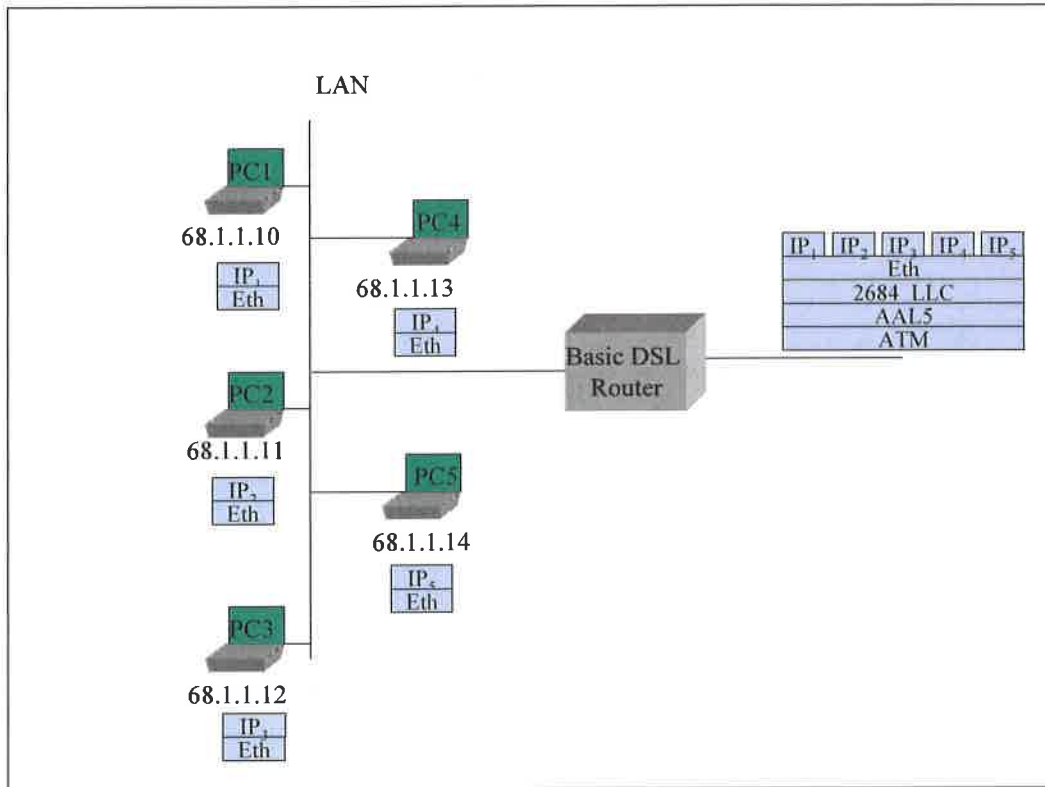
C.3.2 Router in Bridged Mode, Embedded DHCP Server On

- The router provides a private IP address to each device that it receives a DHCP request from [I - 176].
- The router does not establish any IP or PPP sessions to the WAN.
- No device can get a DHCP response from the WAN, since the router will intercept all DHCP requests that come to it.
- PC1 and PC3 each use a PPPoE client to establish their own PPPoE sessions [I - 137, I - 140]. While the private IP address from the router is still associated with their PC Ethernet interfaces, PC1 and PC3 also have a public IP address associated with their respective PPPoE interfaces. Common behavior is for all IP traffic of PC1 and PC3 to now use their own PPPoE interfaces.
- PCs that do not establish their own PPPoE connection cannot connect to the WAN, but they can communicate with other PCs on the LAN.



C.3.3 Router in Bridged Mode, Embedded DHCP Server Off

- The router does not establish any IP or PPP sessions to the WAN.
- All DHCP requests are bridged on to the WAN [I - 107].



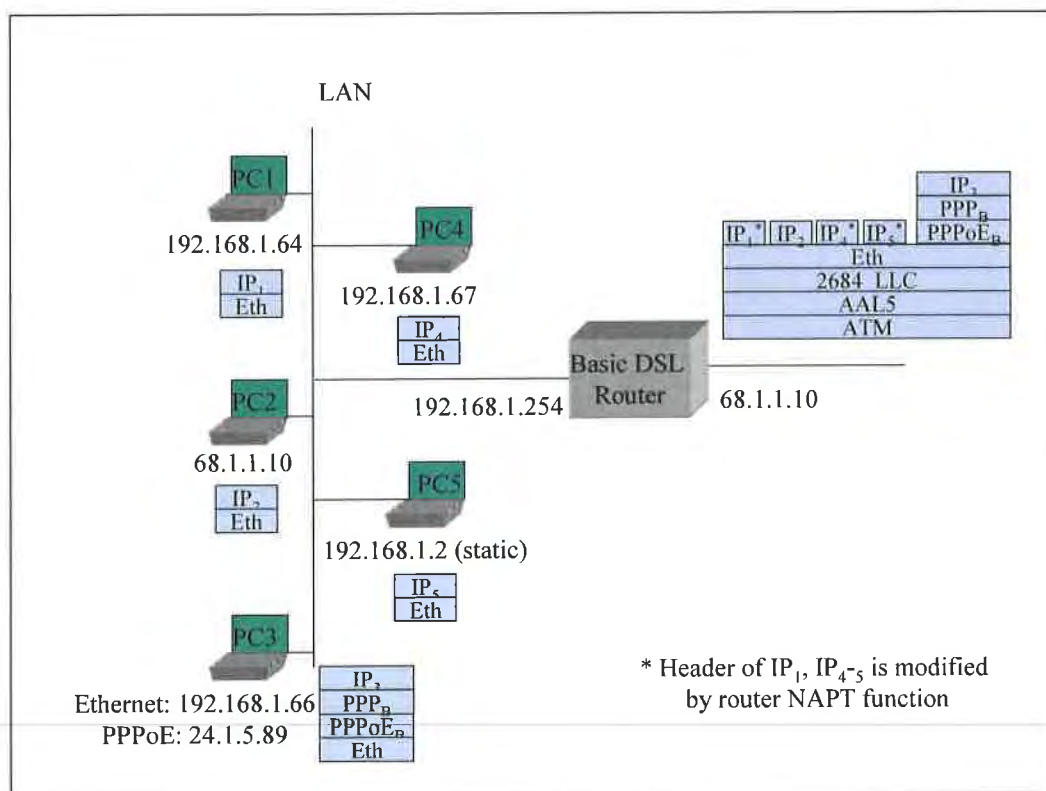
C.4 Simultaneous IP and PPPoE WAN Sessions

TR-059 requirements have PPPoE and IP sessions running simultaneously over the same PVC. Here are some examples of how this might look, assuming the network is capable of terminating PPPoE and IP at the same time on the same PVC.

Note: Simultaneous IP and PPPoE is not well supported in the network today. Most equipment terminating the ATM PVC does not support both IP and PPPoE connections at the same time.

C.4.1 Router in IP-routed “2684 Bridged” Mode, Embedded DHCP Server On

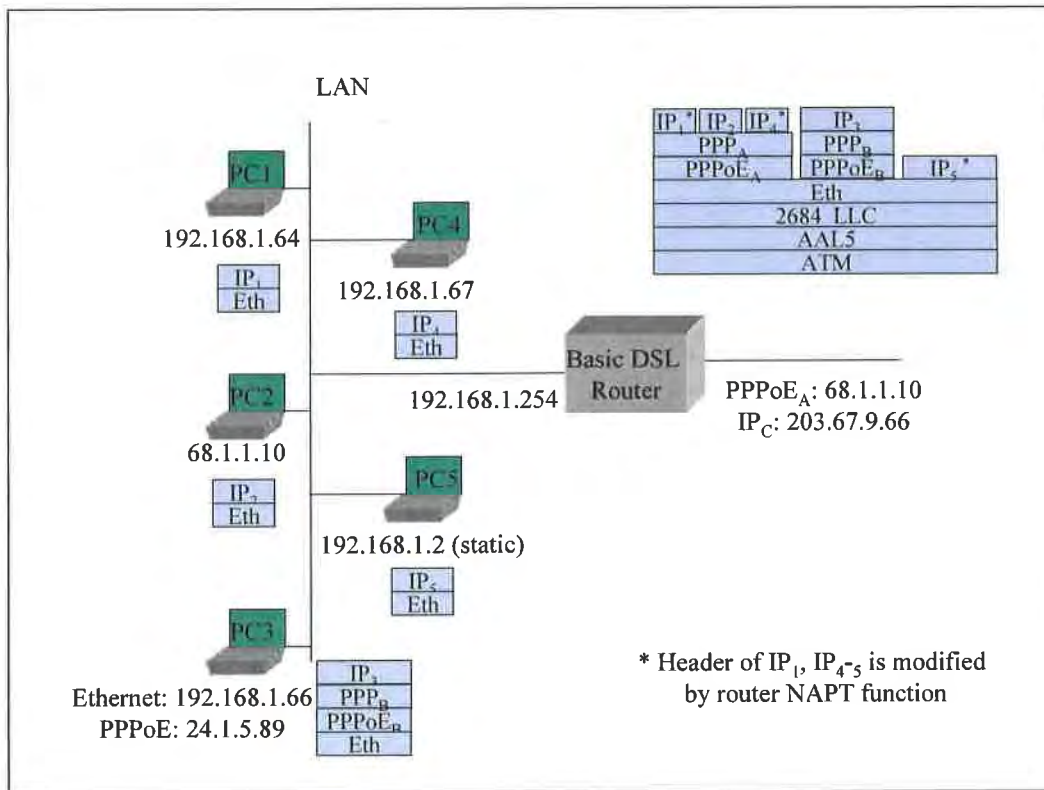
- The router provides an IP address to each device that it receives a DHCP request from.
- PC5 uses a static IP address and does not send a DHCP request to the router.
- The router has been configured to give PC2 its WAN address. When the router has no WAN connection, it gives PC2 a private address with a 10 minute lease time.
- The router issues a DHCP request and establishes an IP session to the WAN.
- The router gives its public IP address to PC2.
- PC3 uses a PPPoE client to establish its own PPPoE session [I - 137, I - 140]. While the private IP address from the router is still associated with PC3’s Ethernet interface, PC3 also has a public IP address associated with its own PPPoE interface. Common behavior is for all IP traffic of PC3 to now use this PPPoE interface.



C.4.2 Router Sets Up IP as a Second Session

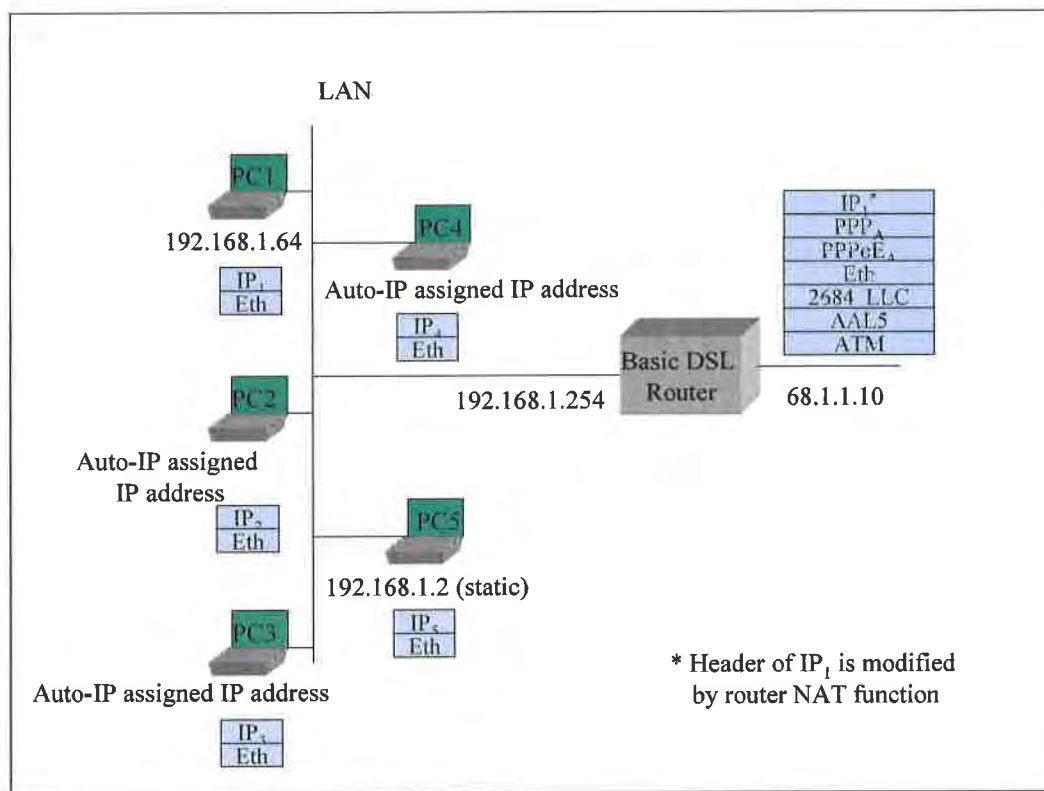
Assuming the scenario in section C.2.3 as a base, add:

- The router sets up connection IP_C [I - 121]. It gets an IP address and DNS addresses through a DHCP client request. It gets routing information from RIP-2 [I - 210]. PPPoE_A remains the default route.
- PC5 requests a DNS lookup for a URL. The router sends simultaneous URL lookup requests to DNS servers on both connections. The DNS server on the PPPoE_A connection fails to resolve the URL and the IP_C connection returns an IP address. The router returns the IP address to PC5 [I - 230].
- PC5 sends IP packets to the returned IP address. The router determines from its routing table that this goes to connection IP_C.



C.5 Single PC Mode of Operation

- The router is configured to use the single PC mode of operation [I - 202].
- The router's embedded DHCP server is on. The embedded DHCP server has only one address lease available in this case.
- PC1 is the first device seen, so it is identified as the “single PC”.
- PC1 is provided with a private IP address and 1:1 NAT is performed between the WAN and PC1 by the router. The subnet mask sent to PC1 is 255.255.255.0.
- Alternately PC1 could be given the router’s public address instead, as with PC2 in the scenarios in Section C.2.



C.6 Router Embedded DHCP Server Gives Out Public IP Addresses (from use of IPCP extension)

- The router initially gives private IP addresses to PCs, before setting up its PPPoE session.
- The router sets up PPPoE to ISP and gets IP address and DNS server addresses via IPCP. It also gets a subnet mask via an IPCP extension [I - 171, I - 172].
- The router gives public IP addresses to certain PCs when they issue DHCP requests again [I - 201].
- PC5 is set for static IP and does not issue a DHCP request.

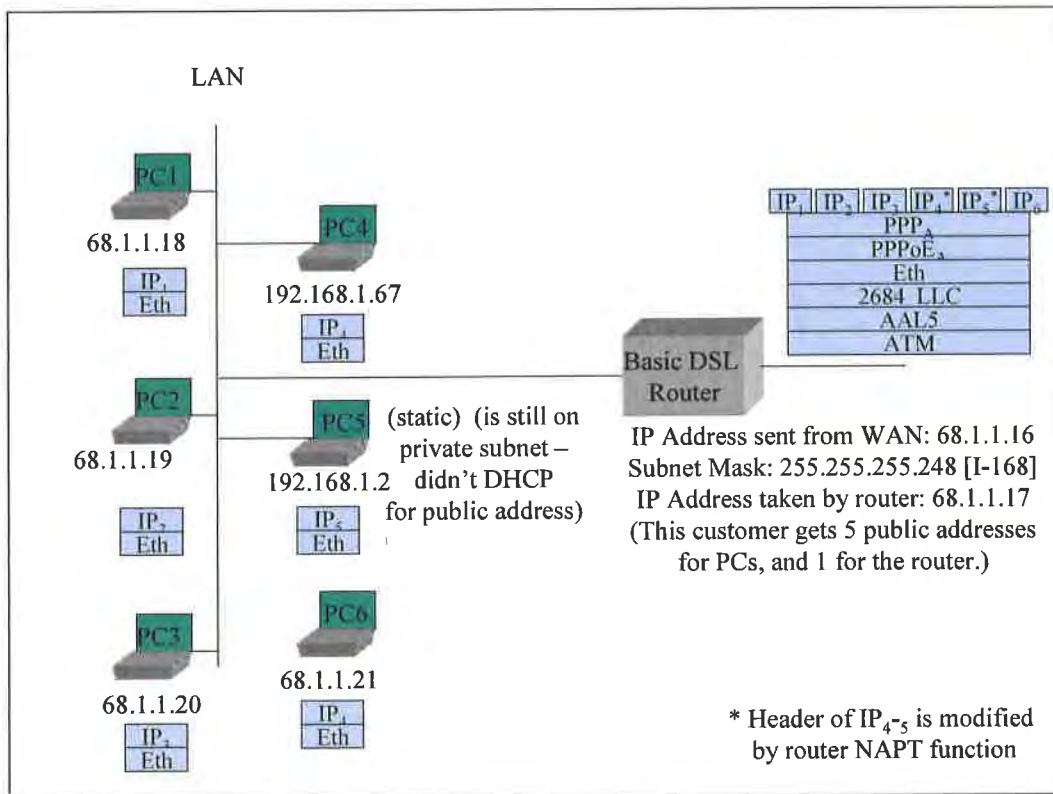


EXHIBIT A

http://web.archive.org/web/20050131032255/http://www.dslforum.org/aboutdsl/Technical_Reports/TR-094.pdf

Technical Report

DSL Forum

TR-094

Multi-Service Delivery Framework for Home Networks

August 2004

Produced by:
The Architecture and Transport Working Group
&
DSL Home Technical Working Group

Editor:
Mark Dowker, Bell Canada

Architecture and Transport Working Group Chairs:
David Allan, Nortel Networks and David Thorne, BT

DSLHome Technical Working Group Chairs:
Greg Bathrick, Texas Instruments, George Pitsoulakis, Westell

Notice:

The DSL Forum is a non-profit corporation organized to create guidelines for DSL network system development and deployment. This Technical Report has been approved by members of the Forum. This document is not binding on the DSL Forum, any of its members, or any developer or service provider involved in DSL. This document is subject to change, but only with approval of members of the Forum.

©2004 Digital Subscriber Line Forum. All Rights Reserved.

DSL Forum technical reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only.

Notwithstanding anything to the contrary, the DSL Forum makes no representation or warranty, expressed or implied, concerning this publication, its contents or the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by the DSL Forum as a result of reliance upon any information contained in this publication. The DSL Forum does not assume any responsibility to update or correct any information in this publication.

This page intentionally left blank.

Document History

Revision History	Date	Reason for Update
Version 1.0	November 2003	Initial document distributed for discussion.
Version 2.0	December 2003	Incorporated QoS change for HomePlug 1.0 based on contribution DSL2003.460.00 reviewed in Paris
Version 3.0	March 2004	Incorporate changes based on contributions (2004.022 & 2004.056 & 1 exploder change) received up to the Brussels meeting.
Version 4.0	Jun 2004	<ul style="list-style-type: none">• Incorporate editorial updates and changes to resolve comments received from the straw ballot process. See contributions: 2004.140, 2004.144, 2004.145, 2004.146, 2004.166, 2004.179 and 2004.194.• Updated WT numbers to new TR numbers as follows:<ul style="list-style-type: none">○ WT-082 → TR-64○ WT-086 → TR-68○ WT-087 → TR-69

This page intentionally left blank.

Table of Contents

1	SCOPE AND PURPOSE	1
1.1	INTRODUCTION	1
1.2	PURPOSE	1
1.3	SCOPE	2
1.4	RELATION TO OTHER STANDARDS AND FORUMS	2
1.5	REQUIREMENTS	3
1.6	HOME NETWORKING ARCHITECTURE GOALS	3
1.7	ASSUMPTIONS	3
2	APPLICATIONS AND SERVICES	5
2.1	VOICE	5
2.2	VIDEO	5
2.2.1	Digital Broadcast Video	5
2.2.2	Non-traditional Video	5
2.2.2.1	Internet Video	5
2.2.2.2	Video on Demand (VoD)	6
2.2.2.3	Video Conferencing	6
2.2.2.4	Remote Education	6
2.2.3	Digital Video & the DSL Based Home Network	7
2.2.3.1	The Analog Split-off	7
2.2.3.2	End to end Digital Video	7
2.2.3.3	Hybrid (Combo-box)	8
2.2.3.4	Digital Media Server/Receiver	8
2.3	DATA	10
2.3.1	Web Browsing/Internet Sharing	10
2.3.2	File and Peripheral Sharing	10
2.3.3	Game Consoles	10
2.3.4	Remote Telemetry & Control	10
3	HOME NETWORK OPERATIONAL FUNCTIONALITY	11
3.1	EXTERNAL CONNECTIVITY	11
3.2	INTRA-HOME CONNECTIVITY	11
3.3	QOS AND THE HOME NETWORK ARCHITECTURE	12
3.3.1	WAN QoS	13
3.3.2	Home Network QoS	13
3.4	PROVIDE A "PLUG IT IN AND IT WORKS" USER EXPERIENCE	14
3.5	STORAGE	14
3.6	DEVICE POWERING	15
4	HOME NETWORK ARCHITECTURE	17
4.1	THE REFERENCE MODEL	17
4.2	FUNCTIONAL COMPONENTS	17
4.2.1	PS – POTS Splitter	17
4.2.2	B-NT – Broadband Network Termination	17
4.2.2.1	xTU-R	18
4.2.2.2	SM - Service Module	18
4.2.3	RG – Routing Gateway	18
4.2.3.1	PPPoE	18
4.2.3.2	IP Gateway	18
4.2.3.3	QoS Mapping	18

4.2.3.4	Home Network Security	20
4.2.3.5	Management Border Point	20
4.2.4	Premises Distribution	21
4.2.4.1	Distribution Media	21
4.2.4.2	Local Ethernet Switching	21
4.2.4.3	New Network Wiring	22
4.2.4.4	No New Network Wiring	22
4.2.5	FPD – Functional Processing Device	23
4.2.6	EUT – End User Terminal	23
4.2.7	FPD/T – Functional Processing Device and Terminal	24
4.2.8	ASG – Application Service Gateway	24
4.2.9	Supplementary Application Network	24
4.3	INTERFACES	25
4.3.1	U-R Interface	25
4.3.2	U-R2 Interface	25
4.3.3	T _{PDN} Interface	25
4.3.4	T _{CN} Interface	26
4.3.5	R Interface	28
5	HOME NETWORK MANAGEMENT FUNCTIONALITY	29
5.1	HOME NETWORK MANAGEMENT REFERENCE MODEL	29
5.2	DSL ACCESS NETWORK MANAGEMENT	29
5.3	HOME NETWORK MANAGEMENT	29
5.3.1	Service Provider Managed [M] Domain	29
5.3.2	Customer Managed (U) Domain	30
5.4	IP ADDRESS MANAGEMENT	31
5.4.1	RG WAN Side	31
5.4.2	RG LAN Side	31
5.4.3	PPPoE FPD	32
5.5	DOMAIN NAME SERVICES	32
5.6	QUALITY OF SERVICE (QoS)	32
6	HOME NETWORK SECURITY	33
7	GLOSSARY	35
8	APPENDIX A – REFERENCES	39
9	APPENDIX C – PREMISES NETWORK TECHNOLOGIES	41

Table of Figures

Figure 1 - Home Networking Architecture Scope	2
Figure 2 - The Analog Split-off	7
Figure 3 - End to end Digital Video	7
Figure 4 - Hybrid (Combo-box)	8
Figure 5 - Digital Media Server/Receiver	8
Figure 6 - QoS Model for the Home Network.....	13
Figure 7 - The Home Network Functional Architecture	17
Figure 8 - RG Mapping Function	19
Figure 9 - Structured Wiring for Home Networks.....	22
Figure 10 - A Functional Processing Device Example	23
Figure 11 - The Home Network Management Model.....	29

Table of Tables

Table 1 - Home Network Traffic Classes.....	14
Table 2 - End User Terminal Interfaces	28
Table 3 : TV Delivered Applications and Their Traffic Characteristics	41
Table 4 : PC Delivered Applications and Their Traffic Characteristics.....	41
Table 5 : Rate/Reach Distances for Home Networking Premises Distribution Technologies	42

This page intentionally left blank.

1 SCOPE AND PURPOSE

1.1 Introduction

The growth and expansion of high-speed Internet access is undeniable. As more and more consumers consider their high-speed Internet access options, network providers, equipment vendors, and other industry participants want to ensure that the benefits of broadband services are known to consumers, and that customers can easily consume their services where and when they want.

Two characteristics of broadband service technologies that make them an integral part of the home network are: (1) the ability to support multiple logical data connections on the same physical access technology; and (2) the ability to tailor those connections with different qualities of transmission characteristics (i.e., quality of service [QoS]).

Home networking is a phenomenon that has risen in popularity primarily for two reasons: (1) the increasing availability of high-speed Internet access, and (2) the growth in households with multiple PC's. These two drivers combine to create a desire by customers to get the most value from their high speed Internet subscription by connecting multiple devices (usually PC's) to it. Service providers that promote home networking options with their broadband access services will be sought after by customers for information and assistance with setting up and managing their own home networks.

This home networking architecture is proposed in order to facilitate a common understanding of the home environment into which broadband services developed to DSL Forum TR's will be delivered.

1.2 Purpose

The purpose of this working text is to define requirements and capabilities that a home network should provide to take advantage of the full capabilities of multi-service, broadband access services. It also presents a functional home networking architecture that permits multiple residents within the home to use multiple applications and devices with differing connectivity requirements (QoS) and at the same time minimizing poor application performance that could result from conflicting or competing application demands.

This document intends to:

1. Identify some of the applications that the home network will be expected to support in the coming few years.
2. List the functionality that a home network must deliver to meet the application requirements and,
3. Present a reference architecture for a home network that will deliver the above functionality.

The home networking architecture will be defined using functional terms rather than physical devices. By doing so, customers and CPE vendors should be able to create home networks and the related CPE in a way that meets the identified needs and also assures that the resulting home network and equipment will inter-work effectively with the services and applications delivered by the provider broadband (BB) networks.

Multi-Service Delivery Framework for Home Networks.

1.3 Scope

This document presents a reference architecture focused on the home network as it might exist in the residential mass market. It strives to address most aspects of home information technology and applications, with specific attention focused on those aspects that could facilitate the delivery of network-based services and applications. Intra-home applications (i.e., those with no external connectivity needs) are acknowledged, but are generally not explored in-depth.

The potential needs of typical business tele-workers operating at home also are within the scope of the architecture discussion.

The following diagram illustrates the potential scope of this architecture:

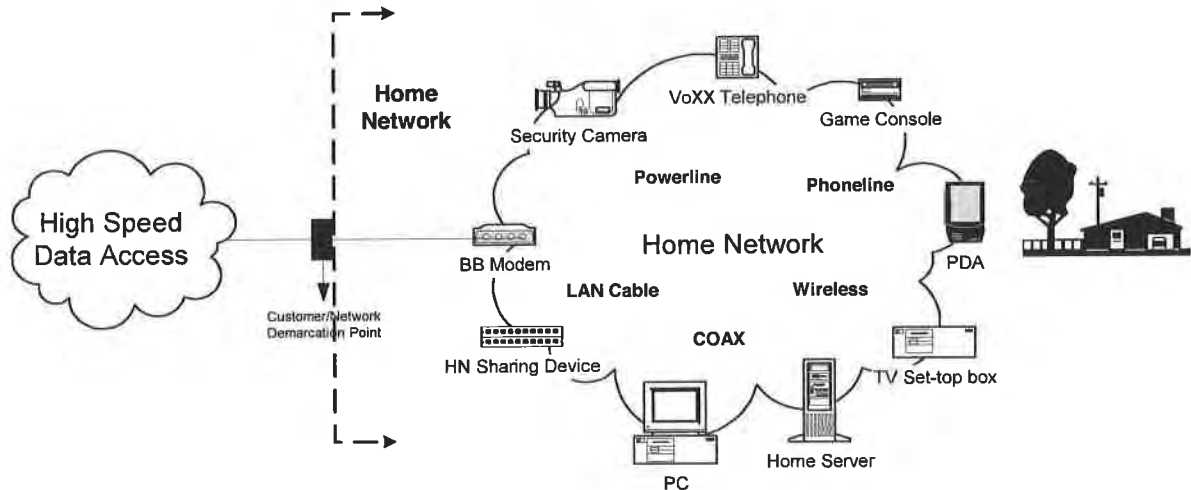


Figure 1 - Home Networking Architecture Scope

Note that while small business networks share many of the attributes of the home network, the architecture discussed in this document might not address all aspects of these small business networks.

1.4 Relation to Other Standards and Forums

Significant work has been done in various standards bodies and industry forums that relates to home networking. One issue with some of this work is that the home network has not been considered as a discrete subject, but rather as part of some other subject. This has led to a fractured view of the home network with some aspects of home networking addressed in one standard and other aspects addressed in another standard, sometimes with conflicting requirements or views.

This document is provided as a complement to other standards and industry efforts that include aspects of home networking. It is intended to provide a high level, integrated view of the home network and identify where the other standards (or portions of standards) apply specifically to the home network.

Multi-Service Delivery Framework for Home Networks.

1.5 Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized and the requirement is preceded by an arrow "→".

- MUST** This word, or the adjective "REQUIRED", means that the definition is an absolute requirement of the architecture.
- MUST NOT** This phrase means that the definition is an absolute prohibition of the architecture.
- SHOULD** This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications must be understood and carefully weighted before choosing a different course.
- SHOULD NOT** This phrase, means that the item should generally be avoided unless valid reasons in particular circumstances warrant including it.
- MAY** This word, or the adjective "OPTIONAL", means that this item is one of an allowed set of alternatives. An implementation that does not include this option **MUST** be prepared to inter-operate with another implementation that does include the option.

1.6 Home Networking Architecture Goals

The following is a list of the goals to be achieved with this home networking architecture.

- Ensure that the home network and its functionality are agnostic to the access technology used to deliver the broadband services and QoS. This permits a wide array of access technologies (e.g., ADSL, ADSL2plus, VDSL, PON) to be used to deliver broadband services to the home and minimizes the impact of changes in the access technology on existing home networking applications.
- Assure interoperability and compatibility with network based services.
- Ensure that the home network and applications take advantage of the benefits delivered by the DSL access. In fact, the home network architecture should be an enabler to delivering multiple applications, both with and without QoS.
- Minimize CPE complexity without sacrificing QoS functionality or flexibility.
- Provide flexibility in the bundling of functions to enable equipment vendors and service providers to provide customers with enticing home network enabled applications tailored to their needs.
- Provide a home network Management capability that is flexible enough to provide a "Plug it in and it works" experience for those customers that choose to have a service provider manage their home network as well as a shared management role between the service provider and the technically savvy customers that wish to take an active role in their home network management.

1.7 Assumptions

- The WAN network services delivered to the home will predominantly be IP and Ethernet based.
- A single broadband data access technology will be used with a particular home network. i.e. one ADSL line, one VDSL line, etc. (This does not preclude the existence of other access technologies into the home [eg. CATV over COAX]).
- The home network will initially be PC centric until wide spread networking capability is built into Consumer Electronic (CE) devices.

EXHIBIT A

2 APPLICATIONS AND SERVICES

This section provides a brief overview of some of the applications that the reference architecture discussed in this document should support.

The following list is not exhaustive, but covers the three primary service areas associated with "Triple Play" of voice, video, and data services.

- Best effort Internet access (Simple Web Surfing)
- Derived voice lines (VoIP based)
- Near Video on Demand - nVoD (store and forward)
- Video on Demand - VoD (streaming video)
- Audio, image and video distribution
- Bandwidth on Demand ("Turbo Button")
- Multiplayer gaming using either PC's or console devices
- Home automation (Telemetry and control)
- Remote Education

2.1 Voice

In addition to the underlying POTS voice services delivered by some DSL technologies, the home network will be required to support additional voice lines derived from the high speed data capabilities of the DSL technologies.

These derived voice services might be offered with few, if any, guarantees (Teen chat over Internet) or with service levels similar to the conventional POTS services. In the case of the latter, the home network will be expected to support some sort of QoS.

2.2 Video

2.2.1 Digital Broadcast Video

Broadcast TV has historically been delivered to a large number of consumers using analog based radio frequency (RF) transmission systems and cable television (CATV) technology. It normally involves re-transmission of video content produced by large television networks as well as independent stations.

Digital Broadcast Video (DBV) replaces the analog CATV technology with digital technology to enable the distribution of broadcast television. In simple terms, the video content is converted to digital format for transmission to the consumer and converted back to analog format in the home for reception on a standard television set. At a minimum, DBV must deliver a customer experience as good as or better than that offered by analog CATV.

There are a number of common ways to deliver the DBV to the consumer. They include modified CATV technology to support digital video, Direct to Home (DTH) satellite transmission and the more recent use of Very high speed DSL technology (e.g., VDSL). Other types of DSL show promise as well.

2.2.2 Non-traditional Video

2.2.2.1 Internet Video

Internet video content commonly found on today's Internet. It is usually delivered in a best effort fashion to a PC running a software player. This is accomplished by streaming the video and other content, whereby the end user can begin to view the content, while it is being downloaded into the computer or other device. The streaming can be delivered via unicast or multicast methods. With unicast, a point to point connection for each receiving device is created. With multicast, a single source stream is replicated by the network to be delivered for each receiving device, reducing the total bandwidth of all sessions.

Multi-Service Delivery Framework for Home Networks.

Examples of typical Internet video content currently include movie trailers, specialty programming, and web cams.

2.2.2.2 Video on Demand (VoD)

VoD provides users with the ability to select video content (usually a movie from a library) and view it at their convenience. It is similar to a video tape being played in a VCR except that the content is delivered via a video distribution technology, instead of from a VCR.

VoD service can be delivered in two primary ways. One is to use IP streaming to deliver the video content in real time to the consuming terminal. Using this type of approach usually requires a better than best effort (BE) QoS from both the WAN and the home network to maintain an acceptable picture quality but it does not require an intermediate staging point.

The second way to deliver video on demand is to use a "download, store, present" model. This involves the best effort download of the video content to a storage device connected within the home network. Once downloaded, the content can be delivered to the consuming terminal. Having the content stored locally significantly reduces the need for the WAN network to support QoS. The need for the home network to support a better relative QoS for the video content depends on whether the content is stored on the same device as is used to deliver it (i.e., a simple video set top box [STB] or a STB equipped with Personal Video Recorder [PVR] capabilities.).

VoD can also be scheduled in the form of live broadcast. Although not a focus of this document, multicast can be accomplished at the ATM layer as well.

2.2.2.3 Video Conferencing

Video conferencing or video telephony permits users to establish point to point connections between their PC's and allow them to see and hear each other as well as share PC data/applications.

R# 1 Home networks **SHOULD** support video conferencing applications.

It is recognized that video conferencing applications normally require symmetrical bandwidth so the home network should provide support for video conferencing applications to the extent permitted by the upstream speed of the access service. This includes supporting any QoS needs of the video conferencing application.

2.2.2.4 Remote Education

Remote education combines both video conferencing and the 2-way interactive data capabilities of the broadband network to create a virtual classroom where students participate remotely with an instructor in a way that mimics a regular class.

Remote education also encompasses the remote access of computer based, multi-media training material.

R# 2 Home networks **SHOULD** support these types of remote education.

Multi-Service Delivery Framework for Home Networks.

2.2.3 Digital Video & the DSL Based Home Network

2.2.3.1 The Analog Split-off

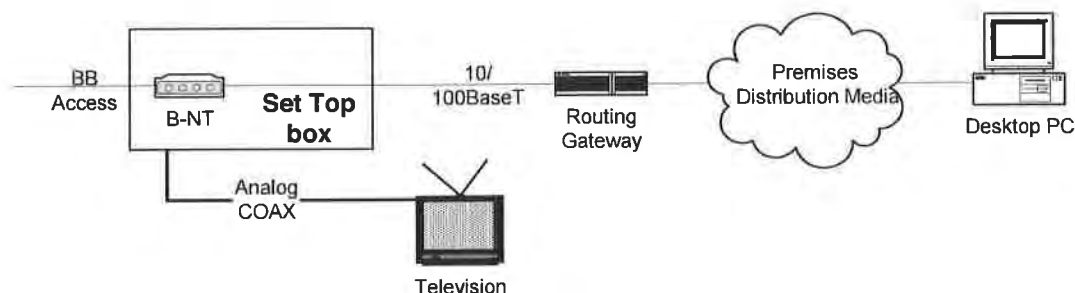


Figure 2 - The Analog Split-off

In this mode of operation, the DBV signals are split and delivered to the television ahead without using the home network to support it. As such, the home network is not required to provide any specific support for the video and hence no special QoS must be supported in the home network to provide an acceptable customer experience.

The analog split-off mode is equivalent to the "Centralized" CPE model described by [5] where the DBV content is converted back to an analog form by a primary set top box and any further distribution of the content (e.g., to other STB's, PC's) is done using analog techniques.

In this configuration, the STB acts as the broadband network termination device for the home network.

The PC could receive some niche video via the Internet connection, but this is normally done today using "best effort" techniques. Evolution towards the QoS enabled home network might hasten the use of the PC as a video presentation device for the DBV stream in addition to the STB.

2.2.3.2 End to end Digital Video

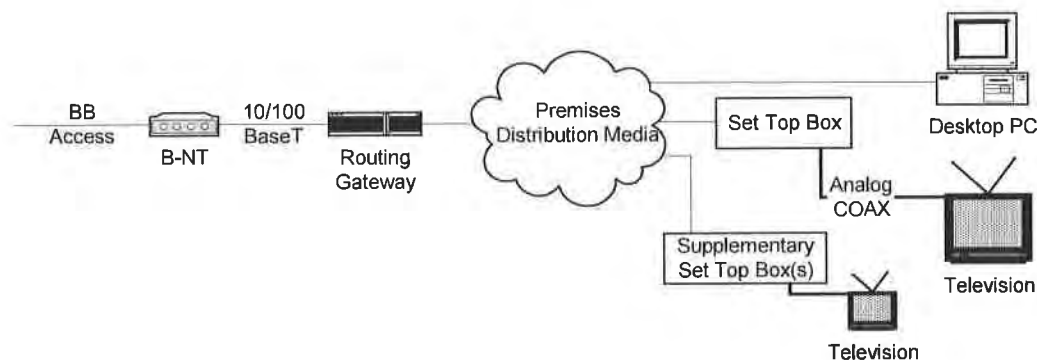


Figure 3 - End to end Digital Video

The end to end digital video configuration sees the home network playing a key role in the delivery of the DBV. In this case, the home network must be able to treat the DBV sessions with a better QoS in order to deliver an acceptable customer experience. The PC will generally continue to receive some niche video via the Internet connection; however the opportunity for the PC to participate in the delivery of the DBV is also possible with this configuration. For example, the PC could use the internal connectivity of the home network to work with the DBV STB to present the DBV content to the PC.

The end to end digital video mode described above is equivalent to the "Distributed" CPE model defined by [5]. The combination of the B-NT and RG replaces the role of the VDSL Termination Processing (VTP) unit in [5] where the DBV content stream is taken from the access and delivered to one or more STB's using a normalized format (commonly Ethernet) via the premises distribution network.

Multi-Service Delivery Framework for Home Networks.

2.2.3.3 Hybrid (Combo-box)

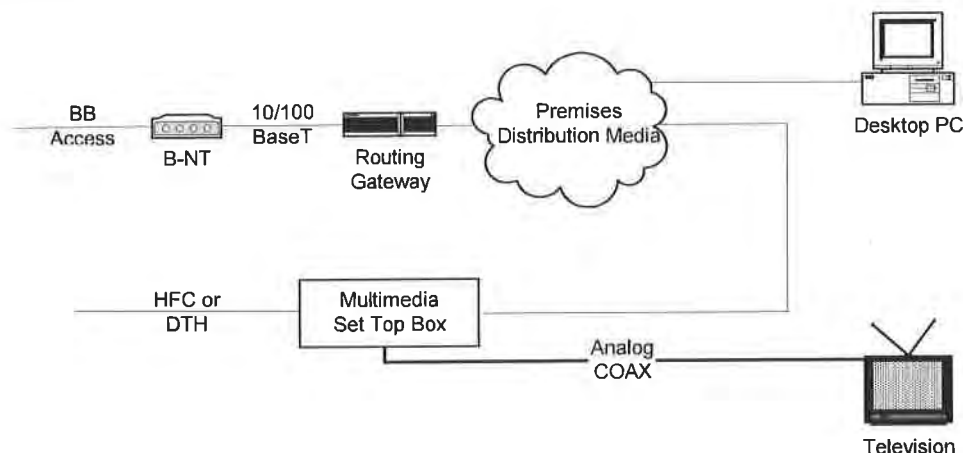


Figure 4 - Hybrid (Combo-box)

The hybrid model sees the DBV (or the analog CATV service) delivered to the home using non DSL access technologies. In this model, the home network supplements the DBV by providing Internet access to a multimedia set top box designed to connect to both the DBV access technology and the home network. This makes it possible for niche video services to be presented on the standard television.

R# 3 The home network **MAY** support different QoS for the niche video if required.

2.2.3.4 Digital Media Server/Receiver

Digital Media Servers/Receivers are becoming more popular as more content becomes available in digital form. Some of the more common digital content includes:

- Images (JPEG's) from digital cameras.
- Audio (MP3's) created from CD's and downloaded from the Internet.
- Video (MOV, WMV, MPEG's) from consumer electronics devices and downloaded from the Internet.

The Digital Media Server/Receiver concept sees a new set of devices connected to the home network that permits digital content to be used throughout the home. The Digital Media Server is a special purpose PC or other device that implements a central repository of digital content. It is connected to the home network and uses the home network connectivity to collect and store the digital content from both local and remote sources.

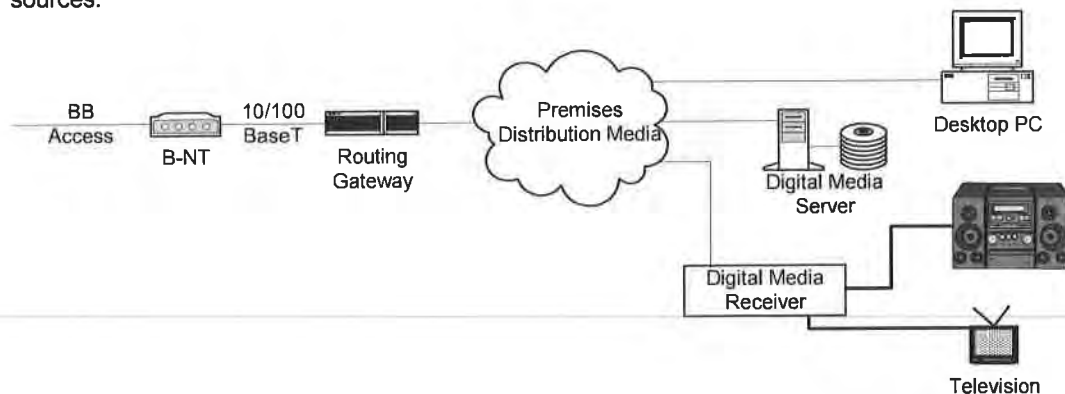


Figure 5 - Digital Media Server/Receiver

Multi-Service Delivery Framework for Home Networks.

Once stored on the Digital Media Server, the content can be accessed by any PC connected to the home network. In addition to using the content with PC's, Digital Media Receivers are now appearing that permit delivering the digital content to more conventional entertainment appliances like stereos and televisions. The Digital Media Receivers are connected to the home network and act as the "bridge" between the home network and the existing home entertainment device.

- R# 4 The home network **MUST** support Digital Media devices with the collection, storage and delivery of digital content from the WAN.

Multi-Service Delivery Framework for Home Networks.

2.3 Data

2.3.1 Web Browsing/Internet Sharing

Web browsing and the desire to share a broadband access among multiple PC's for this purpose have been the driving force behind the creation of home networks. This will continue to be the case.

R# 5 The home network **MUST** support simple web browsing and sharing this capability among multiple PC's in the home.

2.3.2 File and Peripheral Sharing

One of the original purposes for establishing a local area network (LAN) was to provide the ability to share files and other peripherals among the connected PC's. A primary advantage of a home network, in addition to sharing a broadband Internet access, is that the PC's sharing the Internet access can also share files as well as other devices (e.g., printers) attached to the PC.

Once the base connectivity is established for sharing the Internet access, the use of network services within the home network enables the sharing of files and printers. These services have been provided by Network Operating Systems (NOS) in the past and have been absorbed into many of today's operating systems. Examples in use today in home networks include Microsoft Networking and AppleTalk.

R# 6 The home network **MUST** support file and printer network services which allow for sharing and printing among multiple PC's in the home.

2.3.3 Game Consoles

Until recently, PC's have been the primary type of device driving the need for shared Internet access. With broadband access and the ability to share this access in place, other types of devices are appearing that take advantage of the basic data capabilities of the broadband access.

One example is the availability of broadband enabled versions of popular game consoles. Broadband connectivity permits the gaming experience to be enhanced in a number of ways, including (but not limited to):

- Head to head competition with others users outside the home, anywhere in the world.
- New features that are enabled by the broadband capabilities (e.g., voice taunts of your opponent.)
- New games and feature add-ons that can be delivered via the network connection.
- Simplified maintenance of the game console itself though downloadable firmware upgrades.

R# 7 The home network **MUST** support the evolving broadband enabled game consoles and **SHOULD** evolve to provide QoS capabilities that improve the gaming experience.

2.3.4 Remote Telemetry & Control

Home automation involves both remote sensing as well as remote control of various devices within the home. The always connected nature of the broadband access together with a home network makes this possible.

The Open Services Gateway Initiative [OSGi] defines an architecture [7] that enables secure access to remote sensing and control applications within the home. Part of the OSGi architecture includes software functionality at the customer premises that implements the Service Gateway. This Service Gateway uses the external connectivity provided by the broadband access and the home network to provide a secure access to/from the home network.

Note: For the purposes of this home network architecture, the Service Gateway functionality is considered as an application using the connectivity of the home network rather than being a component of the home network itself.

3 HOME NETWORK OPERATIONAL FUNCTIONALITY

The following functional requirements are addressed by this home network architecture.

3.1 External Connectivity

The home network **SHOULD** be able to:

- R# 8 Enable sharing of the BB access within the home by many devices, users and applications.
- R# 9 Provide physical connectivity to the access network for any device connected to the home network. The home network **MUST** provide these components with seamless access to the BB access capabilities (multiple channels, QoS).
- R# 10 Support connectivity to multiple Application Service Providers (ASP's) and Internet Service Providers (ISP's).
- R# 11 Support incoming as well as outgoing access to the Home Network for both customer and service providers.
- R# 12 Provide appropriate QoS delivery from the WAN to and from the home network.
- R# 13 Support IP multicast to the extent needed to permit reception of 1 or more multicast streams by devices within the home network simultaneously.
- R# 14 Be transparent to the applications connected to the home network (e.g., support of SIP sessions for IP telephony, IP VPN transparency).

3.2 Intra-home Connectivity

Intra-home connectivity provides for the interconnection of communicating devices within the customer premises itself. This connectivity supports the more common existing PC based applications (file and printer sharing) and will also begin to play a bigger role as new digital media applications (e.g., those enabled by new IP appliances such as Digital Media Receivers) become popular.

- R# 15 The home network **MUST** support intra-home connectivity.

Most of today's home networking solutions that support intra-home connectivity provide best effort connections only and do not support any QoS or traffic differentiation features. This is due in part to the general availability of economical and relatively high speed LAN (≥ 100 Mbps) switching technologies that make QoS awareness unnecessary for today's applications. As applications evolve and the network demands increase, there will be a need for differentiation of traffic within the home to avoid congestion. With this in mind,

3.3 QoS and the Home Network Architecture

Today's home networks are commonly built using off the shelf technology that consumers purchase from major electronic retailers. The current generation of consumer DSL/Cable routers used in today's home networks are built to be economical for the consumer; however, functionality is sacrificed. Part of the lost functionality is the ability for a home gateway and network to deal with different qualities of service resulting in a home network that supports best effort service only. This hampers the delivery of certain value added applications to subscribers using home networks.

Service Providers and equipment vendors should begin defining and delivering home networking equipment and services that allow their customers to continue realizing the best effort applications they use today but also begin to lay the foundation for new and different applications. One way to do this is to take advantage of the QoS mechanisms of the ATM, Ethernet and IP technologies used to deliver broadband services to deliver extra value to applications running on the home network.

QoS is a nebulous term with many meanings and connotations. This home network Architecture strives to be consistent with the QoS terms defined in section 4.2 of TR-058. The QoS definitions are repeated here for convenience; however the actual TR-058 document should be referenced for current info.

TR-058 QoS Definitions

- ◆ **Quality of Service (QoS)** Quality of Service or QoS refers to the nature of the differentiated traffic delivery service provided, as described by parameters such as achieved bandwidth, packet delay, and packet loss rates. Traditionally, the Internet has offered a Best Effort delivery service, with available bandwidth and delay characteristics dependent on instantaneous load.

There are different types of QoS:
- ◆ **Relative QoS:** This term is used to refer to a traffic delivery service without absolute bounds on the achieved bandwidth, packet delay or packet loss rates. It is used to handle certain classes of traffic differently from other classes;
- ◆ **Guaranteed QoS:** This term is used to refer to a traffic delivery service with certain bounds on some or all of the QoS parameters. These bounds may be hard ones, such as those encountered through such mechanisms as an ATM Call Admission Control (CAC) function or RSVP reservation. Other sets of bounds may be contractual, such as those defined in service level agreements (SLAs) that often typically define a monetary penalty should a certain threshold be crossed or missed.

NOTE: Within this document (and hopefully all derivative documents), the generic terms "QoS" and "QoS on Demand" will be used to describe the general concept of differentiated traffic delivery implemented by means of traffic parameters, without regard to any specific parameter or bound / guarantee. Wherever possible, the qualifying adjectives "Relative" and "Guaranteed" should, at a minimum, be used when describing the needs of a particular service. Ideally, the full definition of the QoS requirements of an application or service should define the various parameters (priority, delay, jitter, etc), any boundaries and the type of boundaries (engineered or contractual) involved.

Figure 6 below illustrates how the above terms relate to the home network. The terms GQoS and RQoS refer to Guaranteed QoS and Relative QoS respectively.

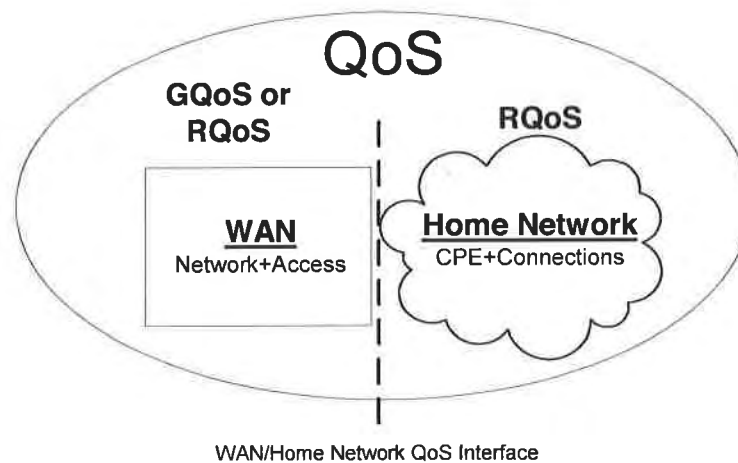


Figure 6 - QoS Model for the Home Network

At the interface between the WAN and the Home Network there will be a function to map between the QoS of the WAN and the relative QoS of the home network. This isolation of the home network QoS from the WAN guaranteed QoS mechanisms will help facilitate migration to full IP QoS in the WAN by insulating the home network applications from the changes in the WAN.

3.3.1 WAN QoS

It is acknowledged that IP will ultimately become a predominant QoS delivery mechanism on the WAN. It is also recognized that significant DSL deployments of ATM based DSL with limited ATM QoS mechanisms are already in place. To address this, the home network architecture defined in this working text will support QoS features independent of the WAN QoS mechanisms (ATM, Ethernet or IP) employed to deliver them.

R# 16 The home network architecture **MUST** support ATM, IP and Ethernet QoS mechanisms used with traffic arriving at and leaving the customer premises.

3.3.2 Home Network QoS

Within the home, the home network's use of relative QoS avoids the need for complex mechanisms and techniques (e.g., subnet bandwidth management, CAC, etc.). The following list summarizes the relative QoS requirements for the home network:

R# 17 The relative QoS within the home network **MUST** be based on the IEEE 802.1q (VLAN) and IEEE 802.1D Annex H.2 (User Priorities and Traffic Classes) standards. Any L3 and above QoS mechanisms will be carried transparently between devices in the home and the routing gateway. Applications operating within the home network may mark IP traffic with different DiffServ code points; however they must encapsulate those IP packets in a tagged Ethernet frame constructed with an appropriate traffic class in the priority field of the IEEE 802.1q VLAN tag.

R# 18 A mapping function between the WAN and LAN QoS's **SHOULD** be employed.

R# 19 Two or more traffic classes **SHOULD** exist in the home network. A "Best Effort" traffic class will always exist and provide the default mode of QoS operation. This ensures backward compatibility with the ad hoc home networks being created by customers today.

R# 20 One or more higher quality traffic classes **SHOULD** exist within the home network.

Multi-Service Delivery Framework for Home Networks.

- R# 21 All devices and applications using these additional traffic classes **MUST** be aware of and behave responsibly within the QoS home network so as to ensure acceptable application performance.
- R# 22 The IEEE 802.1D Annex H.2 priority field **SHOULD** be mapped as defined in CEA-2007. This standard creates four types of QoS that can operate simultaneously in the same network. The four types are:
1. Best Effort effectively implies that no QoS treatment is applied to traffic marked with this priority.
 2. Prioritized QoS represents traffic with relative QoS. Any prioritized QoS traffic gets better treatment than Best Effort.
 3. Parameterized QoS represents traffic that requires a guarantee of one or more QoS parameters e.g. latency, jitter or packet loss. Parameterized QoS traffic gets better treatment than Prioritized QoS traffic.
 4. Critical QoS is normally reserved for network control messages (channel changes, device mgmt., etc) and not used for content.

Table 1 below illustrates the above grouping and the possible uses for the eight possible priority values. Note: QoS increases moving down the table.

LAN Service Type	LAN Service Level Attributes	Priority Value	Mandatory / Optional	Typical Application	Example Use
Best Effort	No QoS specified. (Default)	000	MUST	No QoS.	Web surfing, FTP, Telnet, Email, device discovery.
Prioritized QoS	Low latency	001	SHOULD	Uni-directional streams.	One way streams for VoD, movies, web cameras.
	Very low latency and low jitter.	010	SHOULD	Real time, bi-directional streams.	VoIP, Video conferencing, gaming.
	Connection control.	011	SHOULD	Stream, session control.	SIP messages, channel changes.
Parameterized QoS	Low latency with target latency specified	100	MAY	Uni-directional streams.	One way streams for broadcast TV, PPV.
	Very low latency and low jitter with latency and jitter parameters specified	101	MAY	Real time, bi-directional streams.	Toll quality VoIP and Video conferencing.
	Connection control.	110	MAY	Stream, session control.	SIP messages, channel changes.
Network Control	Guaranteed delivery	111	MAY	Critical network control and messages to stop network traffic.	Stream/session STOP messages.

Table 1 - Home Network Traffic Classes

Notes:

1. Traffic priority increases from top to bottom with the highest priority class at the bottom.

3.4 Provide a “Plug it in and it works” User Experience

Ideally, all a user sees is a physical jack that the home network device is plugged into and all configuration and set up takes place automatically or with very minimal customer configuration.

3.5 Storage

Storage will become increasingly important as more digital media is created by and for users. The architecture should support the concept of a generic storage function within the home network for storing and accessing various types of digital media. Content could be stored both outside the home network (i.e., in the WAN) and within the home network.

Multi-Service Delivery Framework for Home Networks.

Storage within the home network will have multiple uses. It might act as a content cache to improve performance of a particular application and it could also be applied to longer term storage of user created content such as digital photos, MP3's, documents etc. This content should be accessible to all devices connected to the home network at any time.

R# 23 The home network **SHOULD** support some form of network attached storage for caching and/or long term storage.

3.6 Device Powering

Home network devices and equipment have historically used their own 120/230 VAC power supplies to meet their power requirements. These power supplies could be integrated into the device itself or consist of the power adapters that are commonly supplied with home network devices that plug directly into an AC outlet. The common mode of operation is that these devices usually do not incorporate backup power, leaving the home network and its attached devices susceptible to commercial power outages.

As VoIP services begin to be deployed into the residential consumer environment, there will be increasing demand for the home network and the VoIP terminal devices themselves to operate in a manner similar to today's analog voice services (i.e., continued operation through commercial power outages could be expected).

R# 24 To meet this expectation, the home network **MAY** be required to have a backup power source for both the home network infrastructure itself (i.e., the broadband modem and the LAN switches) as well as provide power to the VoIP terminal devices.

This functionality could be provided by using technology designs that incorporate centralized backup power combined with Power over LAN technologies such as that defined by the IEEE 802.3af standard. The IEEE 802.3af standard describes how to deliver -48VDC power from the central LAN switch over the same Category 5 (Cat 5) cable used for the data connection. This power can then be used by the terminal device, eliminating the time, cost and inconvenience of using separate power cabling, AC outlets and power adapters. Powering of the IEEE 802.3af equipped LAN switch itself using an un-interruptible power source could provide the backup power needs of the LAN infrastructure and the connected VoIP terminal devices.

In cases where the VoIP phone or an adapter does not use a cable that power can be delivered over, other solutions could include batteries within the phone or adapter itself, fallback to an analog mode of operation (as could be possible in the case of HPNA connected devices that are already connected to the phone line) or the use of uninterruptible power supplies to power devices providing VoIP functions such as a VoIP enabled RG.

EXHIBIT A

4 HOME NETWORK ARCHITECTURE

4.1 The Reference Model

The following diagram illustrates the functional components of the DSL enabled home network. The interfaces and components from the DSL Access Network up to and including the SM are in line with the "Customer Premises Specific Reference Model" described in [5]. This home network architecture extends the concepts of TR-61 further into the home network and decouples it from the specific access technology used.

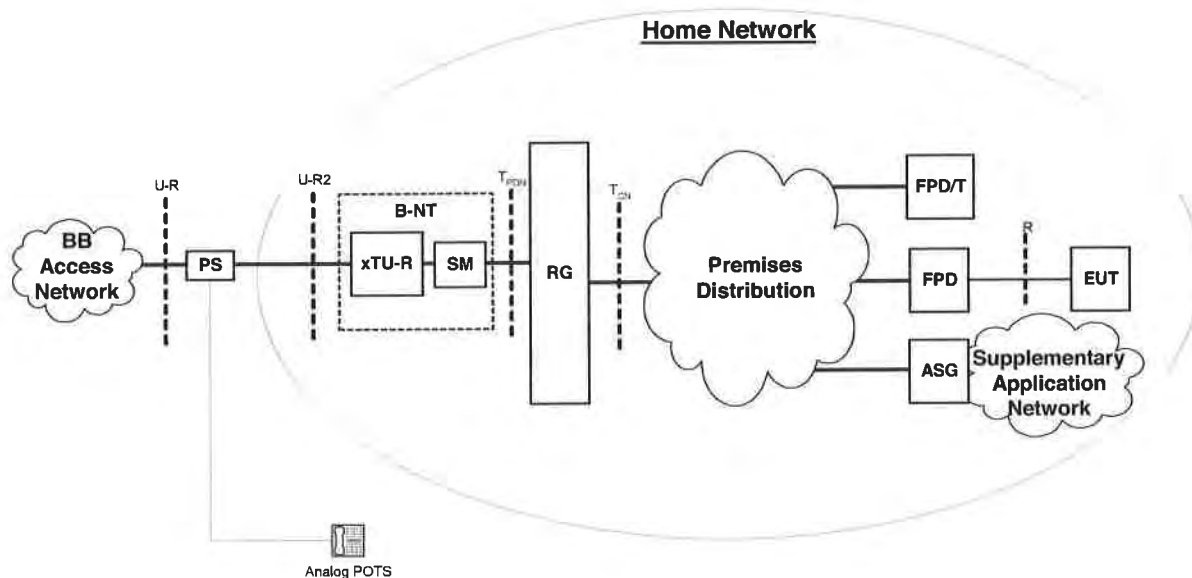


Figure 7 - The Home Network Functional Architecture

4.2 Functional Components

The following section describes in general terms the functions provided by each component of the Home Network Functional Architecture. This is a logical breakdown of these functions. Actual CPE devices could include one or more of these functions. For example, a device might include the B-NT and RG functions while another device might include both RG and ASG functionality.

4.2.1 PS – POTS Splitter

The POTS splitter functionality is used to separate POTS (or N-ISDN) access services from BB access services. The need for splitter functionality is dictated by the specific access technology used. The function could be centralized in one place (centralized POTS splitter) or distributed in the case of distributed filters.

4.2.2 B-NT – Broadband Network Termination

The B-NT is a combination of the xTU-R function and the Service Module (SM) functions described in TR-061. The B-NT physically terminates the specific BB access technology in the home and converts the received digital signals into a single common format for a particular PDN. Today's bridge DSL modems are a good example of the B-NT functionality where the ATU-R and IEEE 802.1D bridge are implemented in a single physical device.

R# 25 The B-NT function **MAY** be integrated with the RG in many products to simplify the implementation and control of QoS between the home network and the DSL access.

When the B-NT is not combined with the RG,

R# 26 The B-NT **MUST** support 10/100BaseT Ethernet toward the home network.

Multi-Service Delivery Framework for Home Networks.

R# 27 The B-NT **SHOULD** implement the WAN side QoS mechanisms and make them accessible via the "T_{PDN}" interface.

4.2.2.1 xTU-R

R# 28 The xTU-R function terminates the BB access line in the customer premises. The specific type of xTU-R function will be determined by the particular access technology used to deliver BB service to the home network.

4.2.2.2 SM - Service Module

The Service Module converts received digital signals into signals suitable for a specific PDN. For the DSL Home Network Architecture the SM processes the digital signals from the xTU-R and presents a single, "normalized" physical and logical interface to the home network via the "TPDN" interface."

4.2.3 RG – Routing Gateway

The RG performs a number of functions described below. Detailed definition of the RG is beyond the scope of this architectural document and will depend on service provider requirements. As such, the definition of specific RG functionality is left for further study and the remainder of this section provides some general RG requirements.

4.2.3.1 PPPoE

R# 29 The RG **SHOULD** support a minimum of one PPPoE termination with the ability to connect directly with a BRAS.

R# 30 The RG **SHOULD** support a capability of initiating multiple PPPoE sessions.

R# 31 The RG **SHOULD** support a PPPoE pass-through capability to permit appropriately featured Functional Processing Devices (FPD) with the ability to connect directly with a BRAS.

4.2.3.2 IP Gateway

The RG is the "traffic cop" between the home network and the broadband access capabilities presented by the B-NT.

R# 32 There **SHOULD** be only one RG function for each home network.
This ensures that the RG is aware of ALL IP traffic into and out of the home network via the DSL access and makes it possible for the RG to perform the next function.

4.2.3.3 QoS Mapping

The RG provides mapping and pass through of all QoS between the WAN and the home network.

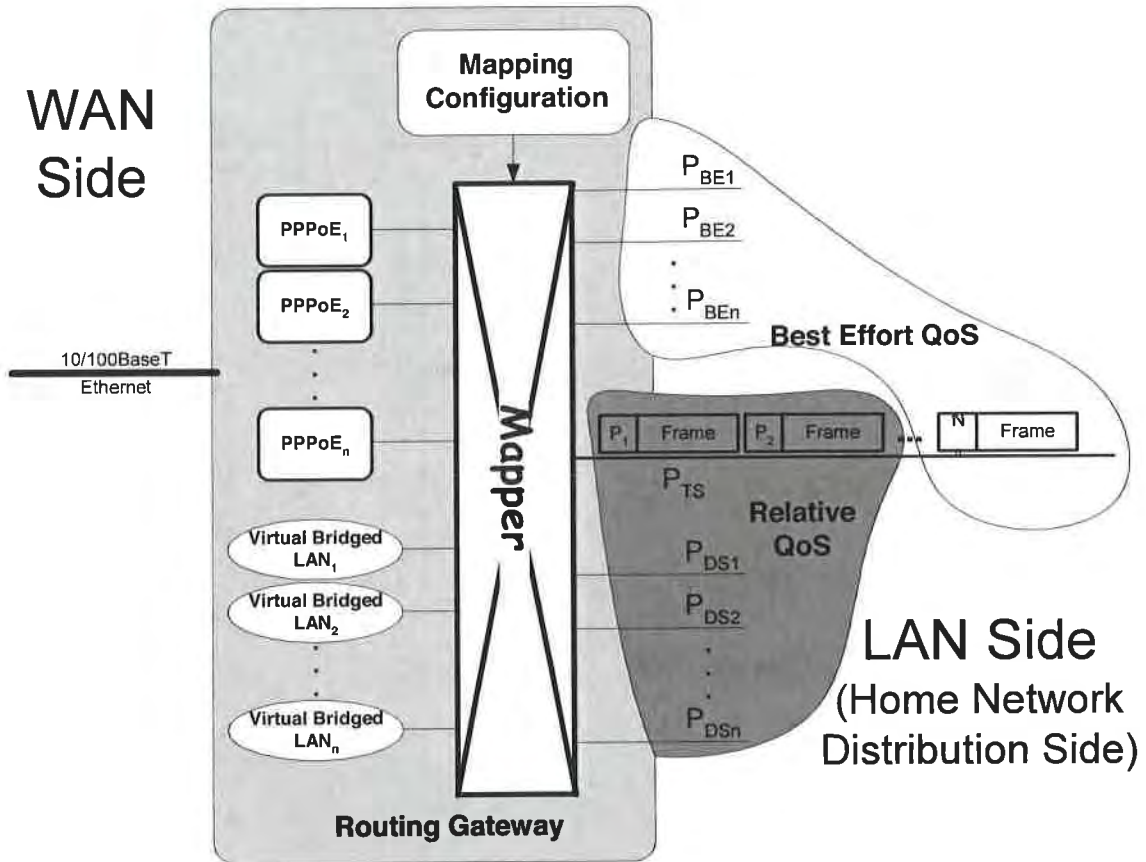


Figure 8 - RG Mapping Function

Figure 8 above shows the generic mapping functionality that the RG provides to support QoS enabled applications.

R# 33 The RG **MUST** implement Relative QoS awareness at layer 2 (IEEE 802.1Q and IEEE 802.1D Annex H) on the LAN side.

R# 34 The RG **SHOULD** implement IP based QoS mechanisms (DiffServ) on the WAN side of the RG.

Implementation of DiffServ in the RG permits it to support IP applications using differentiated services in conjunction with a QoS enabled BRAS.

R# 35 On the LAN side, an RG **MAY** distinguish the different traffic classes using either physical means (i.e., physical ports are mapped to one traffic class) and/or using frame by frame techniques (i.e., using the user priority field of the IEEE 802.1Q VLAN tag).

R# 36 The RG **SHOULD** map between the various Relative QoS services used in the home network and the appropriate QoS enabled virtual channel(s) available from the network. The mapping will be based on one or more characteristics of the data, one being the Relative QoS from the LAN side. The specific policies for doing so will be managed by the access service provider. (See section 5 below entitled "Home Network Management Functionality".)

Multi-Service Delivery Framework for Home Networks.**4.2.3.4 Home Network Security**

R# 37 The RG **SHOULD** provide firewall and network address with port translation (NAPT) capabilities for the home network. When the RG provides these functions, it **MUST** also provide the functions required for applications to work through or across the firewall and the NAPT.

4.2.3.5 Management Border Point

R# 38 The RG should play a major role in the management of the home network. At a minimum, the RG **SHOULD** be involved with:

- LAN+WAN connection mapping
- QoS mapping and policy
- Local IP address management (e.g., DHCP)
- Security configuration

Multi-Service Delivery Framework for Home Networks.

4.2.4 Premises Distribution

The premises distribution function provides the connectivity between the RG and the FPD's. There are numerous technology choices for the premises distribution media, many of which are complex technologies in their own right. The following sections describe various aspects of the premises distribution function.

4.2.4.1 Distribution Media

Examples of premises distribution media that can be utilized for home networking include:

- Category 5 (or better) unshielded twisted pair (UTP) cable.
- Radio Frequency
- AC power electrical wires
- Phone wire
- Coaxial cable
- Multimode Fibre Optic cable

This home networking architecture assumes that multiple premises distribution media can be used to implement the home network connectivity.

4.2.4.2 Local Ethernet Switching

Regardless of the physical media used to make the connection between the RG and the FPD/T, this home networking architecture assumes that all premises distribution technologies are capable of supporting IP packets encapsulated by IEEE 802.3 Ethernet frames. The switching of Ethernet traffic between the various premises distribution media is also a role of the premises distribution function.

- R# 39 The home network **MUST** be capable of supporting IP packets encapsulated by IEEE 802.3 Ethernet frames.
- R# 40 Any intra-home connectivity **SHOULD** be implemented using LAN switch technology in order to provide the best possible application performance. Shared media hub devices **SHOULD NOT** be used.
- R# 41 LAN switches used for home networks **SHOULD** provide multiple physical connections for connected devices within the home network allowing the DSL access to be shared by multiple end users and applications within the home.
- R# 42 LAN switches used for home networks **SHOULD** support 10/100BaseT connections and include automatic speed as well as duplex (half or full) negotiation.
- R# 43 Cascading of multiple LAN switches **SHOULD** be avoided to prevent congestion and poor application performance that could result from overloaded "uplink" network segments.
- R# 44 LAN switches for home use **SHOULD** support QoS features.
- R# 45 Any premises distribution technology used to support a L2 QoS aware device **MUST** be capable of providing the necessary support to maintain the distinction between traffic with varying types of QoS.

Multi-Service Delivery Framework for Home Networks.

4.2.4.3 New Network Wiring

The application of network cabling solutions commonly found in business LAN installations can also be applied within the home. These cabling solutions involve “structured” wiring techniques that create a physical hub and spoke design. Figure 9 below illustrates the structured wiring concept.

Structured wiring dictates that a centralized point (hub) be selected on the premises where communication services (i.e., DSL) terminate. Media connectors (typically RJ-45 jacks) are installed throughout the home where required. A cable is then run from each installed connector back to the central wiring point. An Ethernet switch is located at the central wiring point to provide the interconnection of the devices throughout the home.

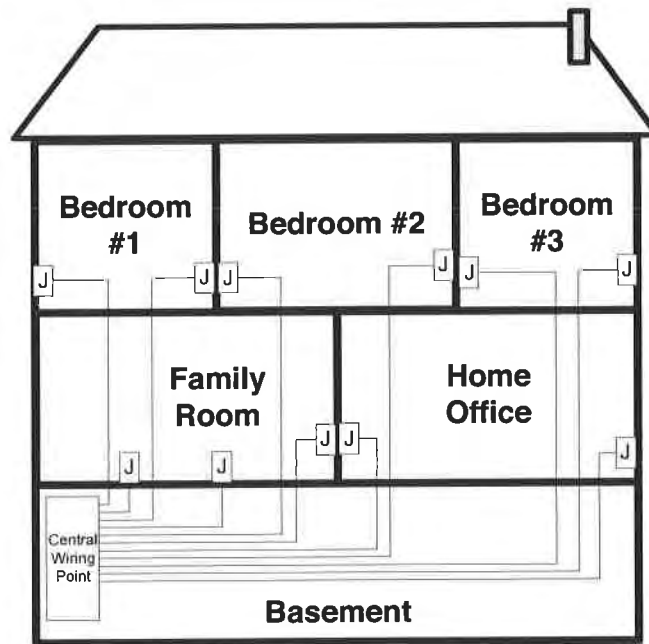


Figure 9 - Structured Wiring for Home Networks

Category 5 (Cat 5) cable is typically used for new structured wiring in a home network. The latest version of Cat 5 is the Cat 5e, although other variations are equally as useful. Cat 5 cabling represents the best option for new home network connections from a QoS perspective. This is due to the relatively high data speeds possible (100 Mbps) and the fact that each connected device has its own dedicated path (not shared with other devices) to the Ethernet switch. These advantages of a structured wiring solution cannot be over-emphasized.

R# 46 Structured wiring **SHOULD** be used for the home network whenever possible.

4.2.4.4 No New Network Wiring

In many situations, practical limitations, both physical and fiscal, exist in the home that preclude the use of standard LAN cabling for connecting devices. In these situations, a number of technology solutions exist to support in-home connectivity for devices without the need to install new wires. The choice of which one to use will depend on the factors that include application needs (especially in the area of QoS), the home environment and the consumer wishes.

Some of the technologies available to avoid the installation of new wiring for the home network include:

- IEEE 802.11x Wireless
- HomePlug™
- HomePNA™

Multi-Service Delivery Framework for Home Networks.

- Data over CATV or Satellite COAX.
(The actual Data over Coax implementation can take one of a number of different forms. These include HomePlug, HPNA & IEEE 802.11 running over the coax in parallel with the analog or digital cable TV signals.)

These technologies can be combined with "local" Ethernet wired connections for total flexibility and best performance. Refer to Appendix C – Premises Network Technologies for example applications and associated physical networking technologies.

4.2.5 FPD – Functional Processing Device

The FPD is a component within the home network that processes voice, video or data for its intended use/application. There can be multiple FPD's within a single home network.

R# 47 All FPD's **MUST** be IP aware and will function as an application specific IP host on the home network. This does not preclude the implementation of multiple FPD entities within a single physical device.

In many cases, the FPD will provide functionality to permit home devices not designed for IP connection to take advantage of network based content and services.

As an example in the figure below, an MP3 player has been designed to permit MP3 source material to be played on the existing stereo system. The material might originate from the Internet or be part of a personal MP3 library that is stored on a PC. The existing stereo receiver has not been designed to connect to the home network but it is the device that the end user normally uses to enjoy music. The MP3 player is the Functional Processing Device in that it is IP aware and processes the MP3 audio material to a form (analog right and left stereo channels) that the stereo receiver can use.

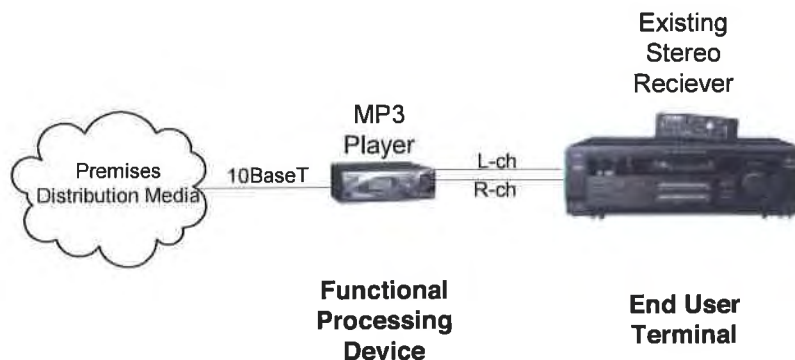


Figure 10 - A Functional Processing Device Example

Other examples of physical devices with FPD functionality include Video Set Top Boxes, streaming audio adapters and VoIP phone adapters for analog phones.

Management of the FPD will be application specific and is outside the scope of the home network architecture.

R# 48 The connectivity services provided by the home network and broadband access **MAY** be used by the application to manage the FPD.

4.2.6 EUT – End User Terminal

The EUT is a common home appliance that can indirectly take advantage of the home network connectivity but has not been specifically designed to do so. Referring to the previous example of a FPD in Figure 10, the stereo receiver is the End User Terminal. In this example, the stereo can play the analog music

Multi-Service Delivery Framework for Home Networks.

generated by the MP3 player but it cannot be connected directly to the home network. Other examples of EUT's include standard television sets, analog telephones and printers with serial or parallel interfaces.

An EUT will connect to the home network using a FPD as described above.

4.2.7 FPD/T – Functional Processing Device and Terminal

The FPD/T is a FPD used directly by the end user. There is no EUT associated with an FPD/T. Examples include PC's, PDA's, IP Phones, printers with direct network attachment capability.

4.2.8 ASG – Application Service Gateway

It is recognized that there are and will continue to be non-IP based networks within a home. Examples include home automation networks based on technologies like Lonworks, CEBus, X.10 networks, IEEE 1394 Firewire and even analog based key telephone systems. Home entertainment system components can also be connected together with proprietary links for control purposes.

An ASG is a special instance of a FPD that acts as a gateway between the IP/QoS enabled home network defined by this architecture and these non-IP aware networks. As identified in Section 4.2, the ASG may be implemented in the same physical device as the RG or as a separate physical device.

The OSGi Service Gateway [7] is an example of an ASG device implemented on the home network with the external (WAN) connectivity and associated QoS provided by the home network.

4.2.9 Supplementary Application Network

Supplementary networks, specific to certain applications will exist within the home. The goal of this architecture is to recognize the existence of these networks and to provide these networks and their applications with access to the functionality provided by the home network as described in section 3 - Home Network Operational Functionality. Examples of some supplementary application networks include today's home security, climate control and telemetry systems. Home networking support of these supplementary networks will be via an ASG.

R# 49 The ASG **MAY** support a Home Distribution function running in addition to the Premises Distribution function already supported by the Home Network. In addition, the Supplementary Application Network **MAY** utilize the Premises Distribution network if the latter supports transport of non-IP traffic."

Multi-Service Delivery Framework for Home Networks.

4.3 Interfaces

This section describes the interfaces between the functional components of the home networking architecture as illustrated in Figure 7 - The Home Network Functional Architecture.

Some of the sub-interfaces of the U, T and R interfaces, might not be physically discernable, as they could be integrated within home network devices. Examples of sub-interfaces are U-R, U-R2, T_{PDN}, and T_{CN}. In cases where the sub-interfaces are not discernable, the interface is comprised of the union of the individual sub-interface definitions.

4.3.1 U-R Interface

This is the interface presented by the specific access technology towards the customer premise. In most instances, it will be from the customer side of the customer/network demarcation device. The interface will take different forms depending on the access technology used to deliver the service. Some examples are:

- Single copper pair running ADSL
- Single copper pair running VDSL
- Single fibre running PON

R# 50 The B-NT **MUST** terminate at a single broadband U-interface.

4.3.2 U-R2 Interface

The U-R2 interface will be present in situations when the access technology delivers broadband and POTS access services on the same physical media. In cases where the access technology is dedicated to broadband access only (i.e., no POTS service is supported), the U-R and U-R2 interfaces are one and the same. No splitter is required in these circumstances.

4.3.3 T_{PDN} Interface

The T_{PDN} interface is physically discernable when the B-NT and RG are implemented in separate devices.

R# 51 In these situations, the TPDN interface **MUST** be limited to being a point to point layer 1+2 connection between the RG and the B-NT.

Use of shared media hubs in conjunction with this interface is discouraged. This will ensure that the RG has knowledge of the total traffic between the home network and the B-NT and permit the RG to maintain the integrity of the QoS for the external connections.

When present, the T_{PDN} interface has the following characteristics:

Data Link Layer

R# 52 The data link layer **MUST** support Ethernet in accordance with IEEE 802.2/ IEEE 802.3 (Ethernet)

R# 53 The data link layer **MUST** support the bidirectional delivery of PPP over Ethernet frames in accordance with IETF RFC 2516.

R# 54 The data link layer **MUST** support the operation of DHCP.

R# 55 The data link layer **SHOULD** support Ethernet virtual LANs (IEEE 802.1Q).

R# 56 The data link layer **SHOULD** support Ethernet precedence of LAN traffic (IEEE 802.1D Annex H).

Multi-Service Delivery Framework for Home Networks.

R# 57 The data link layer **SHOULD** support the bidirectional delivery of IP packets.

Logical Link Controller (LLC) Sublayer

R# 58 The logical link controller sublayer subinterface **MUST** support Ethernet in accordance with IEEE 802.2.

Medium Access Control (MAC) Sublayer

R# 59 The medium access control sublayer subinterface **MUST** support Ethernet in accordance with IEEE 802.3.

Physical Layer

R# 60 The physical layer for the TPDN interface **MUST** be a 10/100BaseT interface, using an RJ45 connector.

R# 61 The TPDN interface **MUST** support the automatic negotiation of the speed without customer intervention.

R# 62 The TPDN interface **MUST** support full duplex operation to ensure that traffic in the downstream or upstream direction does not affect traffic in the opposite direction.

4.3.4 T_{CN} Interface

The T_{CN} Interface defines the interface between the RG and the various premises distribution technologies.

R# 63 There **MUST** be a minimum of one TCN interface presented by an RG for connection to the premises distribution network.

The above does not preclude an RG device from integrating premises distribution functions as described in section 4.2.4 Premises Distribution; however, at least one such interface must be available.

The T_{CN} Interface will have the following characteristics:

Network Layer

R# 64 The network layer **MUST** support IP version 4 in accordance with IETF RFC 1042.

R# 65 The network layer **SHOULD** support IP version 6 in accordance with IETF RFC 2460.

R# 66 The network layer interface **SHOULD** support IP precedence based on differentiated service (Diffserv) code points in accordance with IETF RFC 3140.

R# 67 The DiffServ requirements defined in TR-059 **SHOULD** be supported.

R# 68 The home network **MUST** support DHCP functions.

R# 69 The home network **MUST** support DNS functions.

R# 70 The home network **MUST** support NAPT functions.

Multi-Service Delivery Framework for Home Networks.

R# 71 The home network **MUST** support UDP and TCP.

Data Link Layer

R# 72 The data link layer **MUST** support Ethernet in accordance with IEEE 802.2/ IEEE 802.3 (Ethernet).

R# 73 The data link layer **MUST** support the transport of PPP over Ethernet frames in accordance with IETF RFC 2516.

R# 74 The data link layer **SHOULD** support Ethernet precedence of LAN traffic (IEEE 802.1Q and IEEE 802.1d Annex H).

Logical Link Controller (LLC) Sublayer

R# 75 The logical link controller sublayer subinterface **MUST** support Ethernet in accordance with IEEE 802.2.

Medium Access Control (MAC) Sublayer

R# 76 The medium access control sublayer subinterface **MUST** support Ethernet in accordance with IEEE 802.3.

Physical Layer

R# 77 The TCN interface **MUST** support 10/100BaseT.

R# 78 The TCN interface **MUST** support both full and half duplex operation.

R# 79 The TCN interface **MUST** support the automatic negotiation of both the speed and duplex without customer intervention.

Multi-Service Delivery Framework for Home Networks.

4.3.5 R Interface

The following table illustrates some of the interfaces that EUT's will present and that an FPD might support to provide connectivity for a particular EUT.

Tip/Ring Telephone line
Ethernet
USB
Coaxial Cable (RF modulated composite video)
S-Video
Composite Video
Component Video
SCART
Dolby Digital/AC-3
L/R Stereo
IEEE 1394
5-channel analogue audio
SCSI
LPDT parallel
RS-232 serial
Bluetooth
IR Emitter (for control of IR controlled devices)

Table 2 - End User Terminal Interfaces

5 HOME NETWORK MANAGEMENT FUNCTIONALITY

5.1 Home Network Management Reference Model

Figure 11 illustrates the management model for the home network. For the purposes of the following discussion, the term “Service Provider” (SP) will be used to refer to either or both an Internet Service Provider (ISP) and an Application Service Provider (ASP).

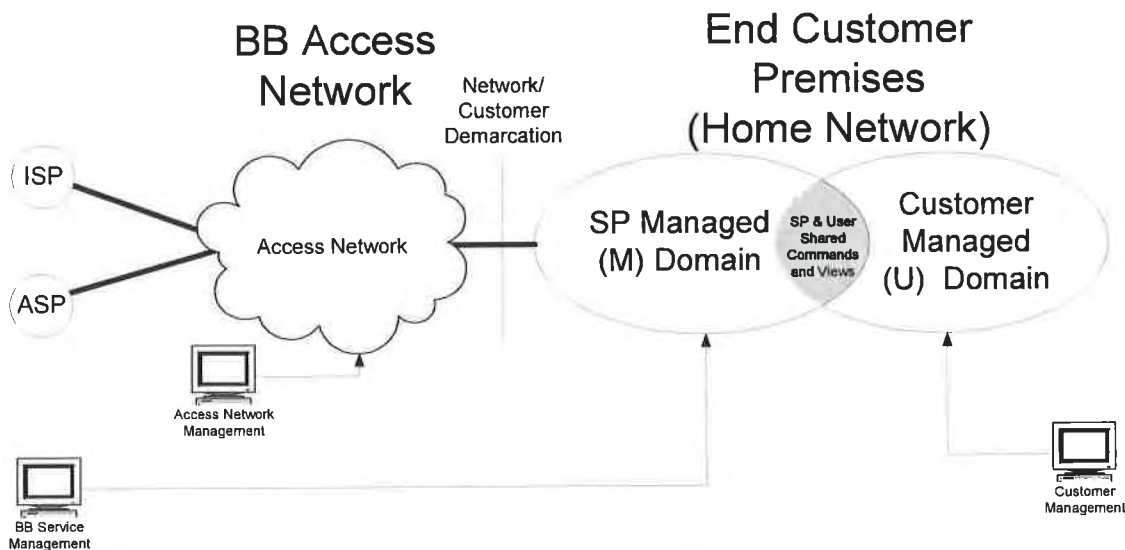


Figure 11 - The Home Network Management Model

5.2 DSL Access Network Management

The BB access network is managed by the provider/operator of the BB access to the home. The focus of this management is on the physical connectivity and switching network between the end customer premises and multiple SP's using the access.

As such, this management is done independent of both the customer and the SP; however, the effects of the management could be monitored by either the customer or the SP. (e.g., a change in the MAX sync speed of the line might be reported by a management entity within the SP or customer managed domains.

The BB management normally stops at the point where the BB access is terminated (the xTU-R) and does not extend into the home network.

5.3 Home Network Management

Management of the home network is a shared activity between the broadband SP and the customer. Figure 11 illustrates this overlap of the home network management responsibilities. The degree of responsibility for management of the home network will be based on an agreement between the customer and the service provider. For example, in cases of a customer purchased device, the customer can enable, disable and control the extent of service provider management of the device, if any. For those cases where a service provider supplies a device as part of the service, the service provider might restrict a customer's ability to manage that device.

5.3.1 Service Provider Managed [M] Domain

The M domain of the home network is part of the more general auto-configuration architecture described in DSL Forum TR-046. With the service provider managed domain of the home network as part of this architecture, the home network can be monitored and controlled by the broadband SP. This allows the broadband SP to configure and support the customer's consumption of their service.

Multi-Service Delivery Framework for Home Networks.

In order to realize this management, devices associated with particular services and connected to the home network, will be accessed by the SP using remote connectivity to some form of back end infrastructure (management servers).

R# 80 Prime aspects of the home network that **MAY** be managed within the M domain include:

- B-NT configuration
- RG configuration including:
 - Connection mapping
 - NAPT configuration
 - QoS policy configuration
- Content security and digital rights management (DRM)
- Home network access security

R# 81 It is anticipated that the RG will be a prime component of the home network involved in the SP management domain. The interaction of the RG with the network **SHOULD** be in line with the recommendations described in DSL Forum TR-69.

5.3.2 Customer Managed (U) Domain

Management within the U domain of the home network is performed either directly by the customer themselves, (e.g., using a management GUI provided by a device) or indirectly by a software "agent" (e.g., a management application running on a PC, driving a LAN management interface like that described in TR-64 or another device discovery and configuration technology such as UPnP™, or Rendezvous™).

In cases where customer management is provided, the home networking devices might present either a management GUI (preferably web based) for direct access by the human client, a software interface (XML based as suggested in [3]) for use by a machine client or both.

Some customer management will be local to the home network only and will not be visible or controllable by the SP. In the case where the service permits some form of customer control/monitoring, user control will be limited to bounds set by the SP. This could be as simple as providing read only access to service configuration/status resident within the M domain or as complex as full user configuration/modification of service attributes within the M domain.

Given the preference for XML based technologies for remote management access within the M domain, it is also preferable to use XML based technologies within the U domain in order to facilitate inter-working between customer and SP management.

R# 82 XML based technologies **SHOULD** be employed within the U domain in order to facilitate inter-working between customer and SP management.

R# 83 Prime aspects of the home network that **MAY** be managed within the U domain include:

- RG configuration including
 - Mapping configuration
 - NAPT configuration
 - IP Addressing
- Home network access security
- Static and dynamic application configuration

Multi-Service Delivery Framework for Home Networks.

5.4 IP Address Management

- R# 84 The home network **MUST** support IPv4 addressing.
- R# 85 The home network **SHOULD** be ready to support IPv6.
- R# 86 When the RG supports bridged connections, IP address assignment for FPD's associated with these connections **MUST** be performed by mechanisms (DHCP, static) from within the ISP or ASP's network.
- R# 87 Any use of private IP addressing **MUST** be done in accordance with [6].

5.4.1 RG WAN Side

On the WAN side of the RG, the following IP address management requirements apply:

- R# 88 The RG **SHOULD** support the following IP address assignment techniques on WAN interfaces:
- o IPCP within PPPoE
 - o DHCP
 - o Static IP configuration
- R# 89 The RG **MUST** accept any and all IP address assignments from the network.
- R# 90 The RG **MAY** be capable of accepting a subnet range of IP addresses from the WAN side for re-assignment to the LAN side of the home network.
- R# 91 When IPv6 support is available, the RG **SHOULD** be capable of accepting a subnet range of IP addresses from the WAN side for re-assignment to the LAN side of the home network.

5.4.2 RG LAN Side

When using routed IP connections, the following requirements apply:

- R# 92 DHCP **MUST** be available for end users to assign addresses for those devices using the routing functions of the RG.
- R# 93 Static IP addresses **SHOULD NOT** be used.
- R# 94 Persistent IP address assignment (i.e., the same IP address is always assigned to a particular device) **SHOULD** be supported because it will be required by some applications.
- R# 95 IP addresses on the TCN side of the RG **SHOULD** be assigned within a default IP address subnet.
- R# 96 A home network **MAY** support multiple IP subnets within itself and the routing between them.

Multi-Service Delivery Framework for Home Networks.

R# 97 In multiple PVC situations where bridged connections could be utilized, FPDs on the home network associated with those bridged connections will be assigned IP addresses from the network. This will normally be done using DHCP.

5.4.3 PPPoE FPD

Some devices will be capable of initiating and supporting their own IP connections using built-in PPPoE functionality. Examples include customer purchased DSL routers and game consoles. IP address assignment will have the following characteristics for these devices:

R# 98 IP addresses **SHOULD** be assigned using IPCP within the device specific PPPoE session by the responding BRAS based on service description (dynamic or persistent).

R# 99 1 IP address **SHOULD** be assigned per PPPoE session initiated.

R# 100 The IP address assigned to the PPPoE FPD **MUST NOT** conflict with any IP addresses on the WAN or LAN side of the RG.

5.5 Domain Name Services

DNS addresses will be communicated as part of the IP address assignment mechanism used for PPPoE enabled devices (RG & PPPoE FPDs). In the case of the RG, it is recommended that the RG act as the DNS server for the default IP subnet.

R# 101 Dynamic DNS update capabilities **MAY** be implemented by RG's and PPPoE enabled FPD's to communicate IP address assignments to Dynamic DNS services.

Any local host naming (i.e., naming of hosts within a private IP subnets) will be left to the customer.

5.6 Quality of Service (QoS)

Quality of service policy configuration will be done on the RG within the SP domain, with or without customer modification from the U domain. This will determine how the RG maps the relative QoS of the home network with the WAN QoS. The actual criteria and policies used to do the mapping are outside the scope of this architecture document. More information on how an RG may implement QoS can be found in [12] and [13].

6 HOME NETWORK SECURITY

The following aspects of security are addressed by devices and applications running on the home network. Together with these devices and applications:

- R# 102 The home network **MUST** provide protection from unwanted connection to the home network from outside. The two main aspects of this include:
1. Undesired connection from the WAN access into the home network as well as restricting specific LAN devices from accessing the WAN. This protection is usually provided by a device providing firewall functions between the home network and the WAN.
 2. Unwanted access to the home network infrastructure itself when that infrastructure includes premises distribution media that are susceptible to unwanted access from outside the home. Examples of these types of media include 802.11 wireless and HomePlug. Protection from this type of unwanted access is achieved by the use of technologies such as the Wired Equivalency Protocol (WEP), Wi-Fi Protected Access (WPA), WPA v2, 802.11i and DES.
- R# 103 The home network **SHOULD** protect against and aid other security functions to protect against the following threats:
1. Trojan horse programs
 2. Back door and remote administration programs
 3. Denial of service
 4. Being an intermediary for another attack
 5. Unprotected Windows shares
- R# 104 The home network **SHOULD** provide protection from unauthorized device configuration from within the home network; either by unauthorized users or rogue software (e.g., Trojan horse applications).
- R# 105 The home network **MAY** provide filtering and parental control of content; however, SP based filtering/control can also be applied.
- R# 106 The home network **SHOULD** support conditional access (CA) and digital rights management (DRM) mechanisms to prevent unauthorized use of content.
- R# 107 The home network **MUST** support remote access VPN clients. This support **MUST** be available to multiple FPD's operating simultaneously on the home network.
- R# 108 The home network **MUST** support the use of encryption both within the home network and toward the broadband network.

EXHIBIT A

7 GLOSSARY

AAA	Authentication, Authorization, and Accounting
AAL5	ATM Adaptation Layer 5
ADSL	Asymmetric Digital Subscriber Line
ADSL2Plus	
AF	Assured Forwarding
API	Application Program Interface
APON	ATM Passive Optical Network
ARP	Address Resolution Protocol
ASG	Application Service Gateway
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
ATU-C	ADSL Termination Unit - Central Office (at Access Network end)
ATU-R	ADSL Termination Unit - Remote (at customer end)
BB	Broadband
BE	Best Effort
B-NT	Broadband Network Termination
BoD	Bandwidth on Demand
BRAS	Broadband Remote Access Server
CA	Conditional Access
CAC	Call Admission Control
Cat5	Category 5
CATV	Cable TV
CBR	Constant Bit Rate
CE	Consumer Electronic
CO	Central Office
COAX	Co-axial cable
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DBV	Digital Broadcast Video
DES	Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
Diffserv	Differentiated Services
DLC	Digital Loop Carrier
DNS	Domain Name Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DTH	Direct to Home
EF	Expedited Forwarding
EPON	Ethernet Passive Optical Network
EUT	End User Terminal
FPD	Functional Processing Device
FPD/T	Functional Processing Device and Terminal
GPON	Gigabit Passive Optical Network
GQoS	Guaranteed QoS
GUI	Graphical User Interface
HFC	Hybrid Fiber Coax
HN	Home Network
HPNA	Home Phoneline Networking Alliance
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange

Multi-Service Delivery Framework for Home Networks.

IP	Internet Protocol
IPCP	IP Control Protocol
IPsec	Secure Internet Protocol
IPv4	IP Version 4
IR	Infrared
ISP	Internet Service Provider
JPEG	Joint Photographic Experts Group
L/R	Left/Right
L2	Layer 2
L3	Layer 3
LAN	Local Area Network
LD	Long Distance
LLC	Logical Link Control
LPDT	Line Printing Data Terminal
MAC	Medium Access Control
MOV	Movie
MP3	MPEG Audio Layer 3
MPEG	Motion Pictures Expert Group
MPLS	Multi-Protocol Label Switching
MTU	Message Transfer Unit
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NG-DLC	Next Generation Digital Loop Carrier
NOS	Network Operating System
NSP	Network Service Provider
nVod	Near Video on Demand
nVoD	Near Video on Demand
OSGi	Open Services Gateway Initiative
PC	Personal Computer
PDN	Premises Distribution Network
PON	Passive Optical Network
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PS	POTS Splitter
PVC	Permanent Virtual Circuit
PVR	Personal Video Recorder
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAM	Remote Access Multiplexer
RF	Radio Frequency
RFC	Request For Comments
RG	Routing Gateway
RQoS	Relative QoS
RSVP	ReSource reserVation Protocol
RT-DSLAM	Remote Digital Subscriber Line Access Multiplexer
SCART	Syndicat des Constructeurs d'Appareils Radiorécepteurs et Téléviseurs
SCSI	Small Computer Systems Interface
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLO	Service Level Objective
SM	Service Module
SONET	Synchronous Optical Network
SP	Service Provider
STB	Set Top Box
SVC	Switched Virtual Circuit
TCP	Transmission Control Protocol

Multi-Service Delivery Framework for Home Networks.

TV	Television
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus
UTP	Untwisted Pair
VAC	Volts Alternating Current
VBR-nrt	Variable Bit Rate - non-Real Time
VBR-rt	Variable Bit Rate - Real Time
VC	Virtual Circuit
VDC	Volts Direct Current
VDSL	Very high speed DSL
VLAN	Virtual Local Area Network
VoD	Video on Demand
VoIP	Voice over Internet Protocol
VTP	VDSL Termination Processing
WAN	Wide Area Network
WEP	Wireless Encryption Protocol
WMV	Windows Media Video
WPA	Wi-Fi Protective Access
XML	Extensible Markup Language

EXHIBIT A

8 APPENDIX A – REFERENCES

- [1] DSL Forum TR-046, "Auto-Configuration: Architecture & Framework"
- [2] DSL Forum TR-058, "Multi-Service Architecture & Framework Requirements"
- [3] DSL Forum TR-059, "DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services"
- [4] DSL Forum TR-064, "LAN-Side DSL CPE Configuration Specification"
- [5] DSL Forum TR-061, "Interfaces and System Configurations for ADSL: Customer Premises"
- [6] DSL Forum TR-069, "CPE WAN Management Protocol"
- [7] FS-VDSL Specification, Part 3, "Customer Premises Equipment Specification"
- [8] IETF RFC 1918, "Best Current Practice - Address Allocation for Private Internets"
- [9] The Open Services Gateway Initiative, "OSGi Service-Platform Release 3" (<http://www.osgi.org/>)
- [10] Consumer Electronics Association, "CEA 2007 QoS Priority Groupings for 802.1Q"
- [11] Consumer Electronics Association, "CEA 2008 Digital Entertainment Network"
- [12] DSL Forum TR-068, "Dual Port ADSL Router Requirements Specification"
- [13] DSL Forum WT-098v2, "Parameter Model Extensions for Service Differentiation"

EXHIBIT A

9 APPENDIX C – PREMISES NETWORK TECHNOLOGIES

The following tables list example applications identified in TR-058 and a rough estimate of the downstream bandwidth required to them. This information can then be used with Table 4 to gauge the appropriate technologies to deploy in a particular environment.

TV Focused Services	Typical bandwidth (downstream)	Service Type¹
Broadcast TV – (e.g., MPEG2)	2 to 6 Mb/s	Parameterized QoS
High definition TV – HDTV	12 to 19 Mb/s	Parameterized QoS
Pay Per View and NVOD (e.g., MPEG2)	2 to 6 Mb/s	Prioritized QoS
VOD – (e.g., MPEG2)	2 to 6 Mb/s	Prioritized QoS
Navigator and EPG (can be locally launched and updated in non real time)	Less than 0.5 Mb/s	Best Effort
Picture in Picture – two MPEG2 channels	Up to 12 Mb/s	Parameterized QoS
Picture in Browser – one MPEG2	Up to 9 Mb/s	Prioritized QoS
Personal Video Records PVR – replay MPEG2 file off hard disk	2 to 6 Mb/s local	Prioritized QoS
ITV - TV telephony features	Less than 64 Kb/s	Best Effort
- TV browser	Up to 3 Mb/s	Best Effort
- TV e-mail	Up to 3 Mb/s	Best Effort
- TV Instant Messaging	Up to 3 Mb/s	Best Effort
- TV Chat	Up to 3 Mb/s	Best Effort
- TV on-screen notification	Less than 64 Kb/s	Best Effort
- TV interactive games	Up to 3 Mb/s	Best Effort
- TV Audio Juke Box	Less than 128 Kb/s	Prioritized QoS

Table 3 : TV Delivered Applications and Their Traffic Characteristics

PC Focused Services	Typical bandwidth (downstream)	Service Type¹
High Speed Internet Access (browsing, IM, Chat, FTP, VPN, access, etc)	Up to 3 Mb/s	Best Effort
Server based E-Mail	As above	Best Effort
Live TV on PC	300 to 750 kb/s	Prioritized QoS
Video on Demand	300 to 750 kb/s	Prioritized QoS
Video Conferencing	300 to 750 kb/s	Prioritized QoS
Voice/Video telephony	64 to 750 kb/s	Prioritized QoS
Interactive Games	10 to 750 kb/s	Prioritized QoS
Remote Education	300 to 750 kb/s	Prioritized QoS

Table 4 : PC Delivered Applications and Their Traffic Characteristics

Notes:

1. Service types are those listed in Table 1 - Home Network Traffic Classes.

Multi-Service Delivery Framework for Home Networks.

The following table shows rough rules of thumb, intended to provide an estimation of how well the different technologies might work in homes. Actual speeds and ranges will vary considerably based on many factors including (but not limited to) vendor selection, installation as well as the caveats included in the "Notes" section.

The last column in the table notes whether a standard to support QoS exists for the networking technology. Even in cases where a technology exists, equipment that supports the QoS standard does not tend to be widely available at this time. It should never be assumed that equipment supports QoS, unless it is explicitly stated.

Technology	Notes	750kbps +	3Mbps+	6Mbps+	9Mbps+	12Mbps	19Mbps	50Mbps+	90Mbps	QoS Standard
100bT Ethernet over CAT5 cable		✓	✓	✓	✓	✓	✓	✓	✓	802.1d Annex H.2
10bT Ethernet over CAT5 cable		✓	✓	✓	✓	No	No	No	No	802.1d Annex H.2
802.11b	1, 4, 7	✓ 40-60m or 3 walls	✓ 30-35m or 1 wall	#, 1 room no walls	No	No	No	No	No	802.11e
802.11g	1, 2, 4, 7	✓ 40-50m or 2 walls	✓ 40-50m or 2 walls	✓ 40-50m or 2 walls	✓ 30-35m or 1 wall	✓ 1 room, no walls	# 1 room, no walls	No	No	802.11e
802.11a	1, 3, 4, 7	✓ 30-35m or 1.5 wall	✓ 30-35m or 1.5 wall	✓ 30-35m or 1.5 wall	✓ 20-25m or 1 wall	✓ 1 room, no walls	# 1 room, no walls	No	No	802.11e
HomePlug 1.0	1, 5, 8	✓	✓	%	No	No	No	No	No	HomePlug QoS mapped to 802.1d Annex H.2
HPNA 2.0	1, 6, 8	✓	✓	%	No	No	No	No	No	for VoHPNA only
HPNA 3.0	1, 6	✓	✓	✓	✓	✓	✓	✓	✓	HPNA3 RQoS+GQoS

Table 5 : Rate/Reach Distances for Home Networking Premises Distribution Technologies

Notes:

- + = speeds shown represent approximate application throughput achievable after physical, link and IP overheads are taken into consideration.
- # = this rate can be achieved in a few homes
- % = this rate can be achieved in a majority of homes
- ✓ = can generally cover an entire average house at this rate
- 1 = claims higher bit rate possible, but that is generally not achievable
- 2 = without 802.11b present
- 3 = 802.11a is not currently allowed outside North America and Japan
- 4 = in chart, wall = regular inside wall; floor = 2 inside walls; outside wall = 4 inside walls
- 5 = assumes not plugged in through surge protector or UPS, circuit not overloaded
- 6 = assumes minimum of CAT3 wiring
- 7 = wireless performance is heavily influenced by materials used in home construction, the position of walls, mirrors, fireplace, closets, furniture, presence of Bluetooth, 2.4GHz phones, microwave ovens, etc.
- 8 = HomePlug and HomePNA have traffic classification features but they are not accessible by applications.

EXHIBIT A

Scientific Atlanta [Login](#) [Search](#) [Sitamap](#)






[Home](#) [Products](#) [Investor Relations](#) [News Center](#) [Contact Us](#) [About Us](#)

WebSTAR User's Guides






Consumers Home
Explorer eClub
FAQs
Downloads

Note: You will need Adobe Acrobat Reader in order to view these documents. Click on the Acrobat Reader graphic to get it if you don't have it.




High Speed Data

-  [DPX100/120 Cable Modem](#)
-  [DPX110 Cable Modem](#)
-  [DPX130 Cable Modem](#)
-  [DPX/EPX2100 Cable Modem](#)
-  [DPC/EPC2100 Cable Modem](#)

Voice over IP (VoIP)

-  [DPX213 VoIP Cable Modem](#)
-  [DPX/EPX2203 VoIP Cable Modem](#)
-  [DPX/EPX2203C VoIP Cable Modem](#)
-  [DPC/EPC2203 VoIP Cable Modem](#)
-  [DPX/EPX2213 VoIP Cable Modem](#)

Home Gateways

-  [DPR362 Cable Modem and Router](#)
-  [DPR/EPR2320 Cable Modem, Router and Wireless Access Point](#)
-  [DPR/EPR2325 Cable Modem Gateway](#)

Home Networking





-  [DPW700 Wireless LAN Adapter PCMCIA Card User's Guide Quick Install Guide](#)
-  [DPW730 USB Wireless Networking Adapter User's Guide Quick Install Guide](#)
-  [DPW939 USB Wireless Networking Adapter User's Guide](#)
-  [DPW941 Wireless Ethernet Adapter User's Guide](#)

EXHIBIT A

©2006 Scientific-Atlanta, Inc. All rights reserved

[Terms of Use](#) | [Privacy Policy](#)

EXHIBIT A

http://web.archive.org/web/20060319045600/http://www.scientificatlanta.com/products/consumers/userguidepdfs/webstar_userguides/4003742.pdf

WebSTAR™ DPR2320™ and DPR2325™ Cable Modem Gateway User's Guide

Introduction

Welcome to the exciting world of digital home and office networking. Your new WebSTAR™ DPR2320™ or DPR2325™ Cable Modem Gateway combines a cable modem, router, and an 802.11g wireless access point in a single device to provide a cost-effective solution for both home and small office networking. This combination allows several users to share one high-speed broadband connection across multiple PCs, laptops, digital cameras, personal data assistants (PDAs), and Internet devices, thereby make sharing files and photos with your family and friends hassle free. With a WebSTAR Cable Modem Gateway, your Internet enjoyment and business productivity will surely soar.

This guide provides procedures and recommendations for placing, installing, configuring, operating, and troubleshooting your cable modem gateway for Internet access and for high-speed wired or wireless broadband networking for your home or office. Refer to the appropriate section in this guide for the specific information you need for your situation. Contact your cable service provider for more information about subscribing to these services.

Benefits and Features

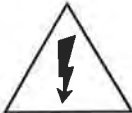



Your new cable modem gateway offers the following outstanding benefits and features:

- Provides a high-speed broadband Internet connection that energizes your online experience, and makes downloading and sharing files and photos with your family and friends hassle free
- Allows you to attach multiple devices in your home or office to the cable modem gateway for high-speed networking and sharing of files and folders without first copying them onto a CD or diskette
- Facilitates high-speed wireless networking of PCs, laptops, and PDAs using the built-in 802.11g wireless access point
- Offers an integrated router (gateway) to simplify setting up a home or office network
- Includes dual antennas (one internal and one external) to provide more uniform wireless coverage in the service area
- Features Plug and Play operation for easy set up and installation
- Provides parental control and advanced firewall technology
- Includes four Ethernet connections (one connection on the DPR2320) and a USB connection for enhanced versatility and flexibility
- Utilizes an attractive compact design that allows for vertical, horizontal, or wall-mount placement
- Allows automatic software upgrades by your cable service provider
- Assures a broad range of interoperability with most cable service providers by complying with Data Over Cable System Interface Specifications (DOCSIS) 1.0, 1.1, and 2.0 standards along with CableHome 1.1 specifications

Notice for CATV Installers

Notice for CATV Installers

If you are a CATV installer, read the information in the box below.

<p>Note to CATV System Installer (USA/Canada Only)</p> <p>This reminder is provided to call the CATV system installer's attention to Article 820-40 of the NEC (Section 54, Part I of the Canadian Electrical Code), that provides guidelines for proper grounding and, in particular, specifies that the CATV cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as practical.</p> <div style="text-align: center;">  </div> <p>This symbol is intended to alert you that uninsulated voltage within this product may have sufficient magnitude to cause electric shock. Therefore, it is dangerous to make any kind of contact with any inside part of this product.</p>	<div style="text-align: center;">  </div> <div style="text-align: center;"> <table border="1"> <tr> <td>CAUTION</td> </tr> <tr> <td>RISK OF ELECTRIC SHOCK DO NOT OPEN</td> </tr> <tr> <td>AVIS</td> </tr> <tr> <td>RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR</td> </tr> </table> </div> <div style="text-align: center;">  </div> <p>CAUTION: To reduce the risk of electric shock, do not remove cover (or back). No user-serviceable parts inside. Refer servicing to qualified service personnel.</p> <p>WARNING TO PREVENT FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS UNIT TO RAIN OR MOISTURE.</p> <div style="text-align: center;">  </div> <p>This symbol is intended to alert you of the presence of important operating and maintenance (servicing) instructions in the literature accompanying this product.</p>	CAUTION	RISK OF ELECTRIC SHOCK DO NOT OPEN	AVIS	RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR
CAUTION					
RISK OF ELECTRIC SHOCK DO NOT OPEN					
AVIS					
RISQUE DE CHOC ÉLECTRIQUE NE PAS OUVRIR					

In This Guide

IMPORTANT SAFETY INSTRUCTIONS	4
What's In the Carton?	7
DPR2320 Front Panel Description	8
DPR2320 Back Panel Description	9
DPR2325 Front Panel Description	10
DPR2325 Back Panel Description	11
Where is the Best Location for My Cable Modem Gateway?	12
What are the System Requirements for Internet Service?	12
How Do I Set Up My High-Speed Internet Access Account?	13
How Do I Connect My Devices to Use the Internet?	14
How Do I Configure TCP/IP Protocol?	16
How Do I Install USB Drivers?	19
How Do I Troubleshoot My Internet Service Installation?	21
What are the Requirements for Ethernet Network Devices?	23
How Do I Select and Place Ethernet Network Devices?	24
How Do I Connect Ethernet Network Devices?	25
What are the Requirements for USB Network Devices?	27
How Do I Select and Place USB Network Devices?	28
How Do I Connect USB Network Devices?	29
What are the Requirements for Wireless Network Devices?	31
How Do I Select and Place Wireless Network Devices?	32
How Do I Install Wireless Network Devices?	33
How Do I Configure the Cable Modem Gateway?	35
Having Difficulty?	92
Tips for Improved Performance	94
How Do I Renew the IP Address on My PC?	95
DPR2320 Front Panel Status Indicator Functions	96
DPR2325 Front Panel Status Indicator Functions	99
Notices	102
FCC Compliance	103
For Information	Back Cover

IMPORTANT SAFETY INSTRUCTIONS

Heed Warnings

Adhere to all warnings on the product and in the operating instructions.

Read, Retain, and Follow These Instructions

Read all of the instructions before you operate this product. Follow all operating instructions that accompany this product. Retain the instructions for future use. Give particular attention to all safety precautions.

Comply With Warnings

Avoid electric shock. Comply with all warnings and cautions in the operating instructions, as well as those that are affixed to this product.

Power Warnings

Providing a Power Source

A label on this product indicates the correct power source for this product. Operate this product only from an electrical outlet with the voltage and frequency indicated on the product label.

If you are uncertain of the type of power supply to your home or business, consult your cable service provider or your local power company.

Grounding This Product (U.S.A and Canada Only)

If this product is equipped with either a three-prong (grounding pin) safety plug or a two-prong (polarized) safety plug, follow these safety guidelines to properly ground this product:

- For a 3-prong plug (one prong on this plug is a protective grounding pin), insert the plug into a grounded mains, 3-prong outlet.

Note: This plug fits only one way. If you are unable to insert this plug fully into the outlet, contact your electrician to replace your obsolete outlet.

- For a 2-prong plug (a polarized plug with one wide blade and one narrow blade), insert the plug into a polarized mains, 2-prong outlet in which one socket is wider than the other.

Note: If you are unable to insert this plug fully into the outlet, try reversing the plug. If the plug still fails to fit, contact an electrician to replace your obsolete outlet.



WARNING:

To avoid electric shock and fire hazard, match the plug and outlet connections carefully, then fully insert. If the plug and outlet do not match, or you cannot fully insert the plug, contact an electrician to update your power outlets.



WARNING:

Avoid electric shock and fire hazard! Do not overload mains AC outlets and extension cords. For products that require battery power or other power sources to operate them, refer to the operating instructions for those products.

Overloading

Do not overload electrical outlets, extension cords, or integral convenience receptacles as this can result in a risk of fire or electric shock. For products that require battery power or other sources to operate, refer to the operating instructions for that product.

Preventing Power Cord Damage

Arrange all power cords so that people or pets cannot walk on the cords. Do not place objects on the cords. Do not lean objects against the cords. Placing objects on or leaning objects against cords can damage the cords. Give particular attention to cords at the point at which the cord connects to plugs, at the electrical outlets, and where the cords exit the product.

Usage Warnings

Providing Ventilation

This product has openings for ventilation that protect it from overheating. To ensure the reliability of this product, do the following:

- Do not block or cover these openings.
- Do not place entertainment devices (such as VCRs or DVDs), lamps, books, vases with liquids, or other objects on top of this product.
- Do not place this product in any of the following locations:
 - On a bed, sofa, rug, or similar surface
 - Near heat sources such as radiators, heat registers, stoves, or other products (including amplifiers) that produce heat
 - In an enclosure, such as a bookcase or rack, unless the installation provides proper ventilation



WARNING:

Avoid personal injury and damage to this product! An unstable surface may cause this product to fall.

Selecting a Proper Location

Place this product in a location that is close enough to an electrical outlet and where the power cord is easily accessible to be disconnected from the wall outlet or from the rear panel of the product.

Important: The power cord is the mains power supply disconnect device.

Place this product on a stable surface. The surface must support the size and weight of this product.

Cleaning This Product

Before cleaning this product, unplug it from the electrical outlet. Use a damp cloth to clean this product. Do not use a liquid cleaner or an aerosol cleaner. Do not use a magnetic/static cleaning device (dust remover) to clean this product.

**WARNING:**

Avoid electric shock and fire hazard! Never push objects through the openings in this product. Foreign objects can cause electrical shorts that can result in electric shock or fire. Do not expose this product to rain or moisture. Do not place objects filled with liquid, such as vases, on this product.

Protecting This Product From Foreign Objects and Water or Moisture Damage

Never push objects of any kind into this product through openings as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock.

Do not expose this product to liquids or moisture. Do not place this product on a wet surface. Do not spill liquids on or near this product.

Do not use this product near water (such as a bathtub, washbowl, sink, or laundry tub), in a wet basement, or near a swimming pool.

Accessories**WARNING:**

Avoid any potential for electric shock or fire. Do not use accessories with this product unless recommended by your cable service provider.

Avoid any potential for electric shock or fire. Do not use accessories with this equipment unless recommended by your cable service provider.

Service Warnings**Servicing This Product**

Do not open the cover of this product. If you open the cover, your warranty will be void. Refer all servicing to qualified personnel only. Contact your cable service provider for instructions.

Obtaining Service for Product Damage

For damage that requires service, unplug this product from the AC outlet. Then, contact your cable service provider or qualified service personnel to obtain service for the following conditions:

- If there is damage to the power-supply cord or plug
- If liquid enters the equipment
- If you drop this product, a heavy object falls on this product, or damage occurs to the cover of this product
- If you expose this product to rain or water
- If this product does not operate normally by following the operating instructions
- If this product exhibits a distinct change in performance

Checking Product Safety

Upon completion of any service or repairs to this product, the service technician must perform safety checks to determine that this product is in proper operating condition.

Lightning

For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet and disconnect the antenna or cable system. This will prevent damage to the product due to lightning and power-line surges. Plugging this product into a surge protector may reduce the risk of damage.

**WARNING:**

Avoid electric shock! Opening or removing the cover may expose you to dangerous voltages. This product contains no user-serviceable parts. Refer all servicing to qualified service personnel.

What's In the Carton?

When you receive your WebSTAR Cable Modem Gateway, you should check the equipment and accessories to verify that each item is in the carton and that each item is undamaged. The carton contains the following items:



One WebSTAR DPR2320 Cable Modem Gateway with detachable antenna



or
One WebSTAR DPR2325 Cable Modem Gateway with detachable antenna



One Ethernet cable (CAT5/RJ-45)



One power adapter with power cord



One USB cable



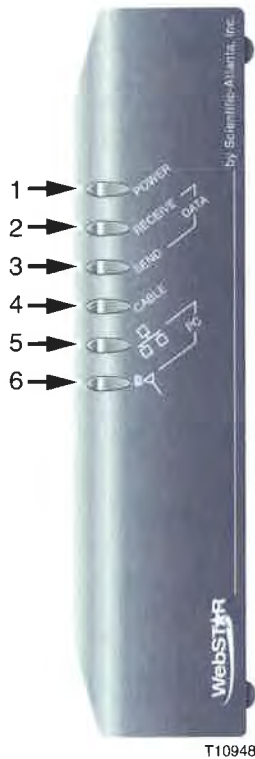
One CD-ROM containing the user's guide and the USB drivers

If any of these items are missing or damaged, please contact your cable service provider for assistance.

You will need an optional cable signal splitter and additional standard RF coaxial cables if you want to connect a VCR, a Digital Home Communications Terminal (DHCT) or a set-top converter, or a TV to the same cable connection as your cable modem.

DPR2320 Front Panel Description

The front panel of your cable modem provides status lights that indicate how well and at what state your cable modem is operating. After the cable modem is successfully registered on the network, the POWER and CABLE status indicators illuminate continuously to show that the cable modem is active and fully operational. See Front Panel Status Indicator Functions, later in this guide, for more information on front panel status indicator functions.

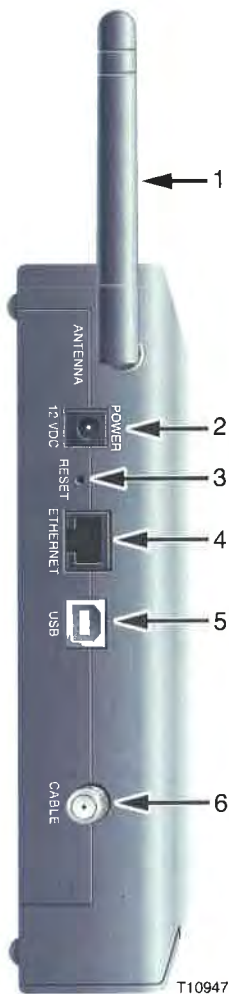


- 1 **POWER**—Illuminates solid green to indicate that power is being applied to the cable modem
- 2 **RECEIVE DATA**—Blinks to indicate that the cable modem is receiving data from the cable network
- 3 **SEND DATA**—Blinks to indicate that the cable modem is sending data to the cable network
- 4 **CABLE**—Illuminates solid green when the cable modem is registered on the network and fully operational. This indicator blinks to indicate one of the following conditions:
 - The cable modem is booting up and not ready for data
 - The cable modem is scanning the network and attempting to register
 - The cable modem has lost registration on the network and will continue blinking until it registers again
- 5 **PC**—Illuminates solid green to indicate that an Ethernet/USB carrier is present and blinks to indicate that Ethernet/USB data is being transferred between the PC and the cable modem
- 6 **PC Wireless**—Illuminates solid green to indicate that a wireless access point is enabled and blinks to indicate that wireless data is being transferred over the wireless connection

Note: After the cable modem is successfully registered on the network, the POWER (LED 1) and CABLE (LED 4) indicators illuminate continuously to indicate that the cable modem is online and fully operational.

DPR2320 Back Panel Description

The following illustration describes the back panel components of the DPR2320.



- 1 ANTENNA— Provides a communication connection for the built-in wireless access point (WAP) to allow wireless devices to communicate with the cable modem
- 2 POWER—Connects the cable modem to the DC output of the AC power adapter that is provided with your cable modem



CAUTION:

Avoid damage to your equipment. Only use the AC power adapter and power cord that is provided with your cable modem.

- 3 RESET—Activating this switch resets the gateway to factory default values and reboots the cable modem



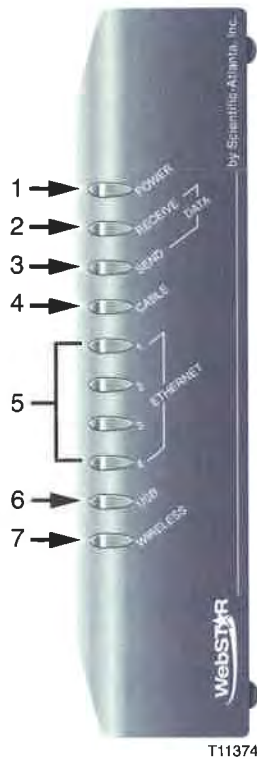
This switch is for maintenance purposes only. Do not use unless directed to do so by your service provider.

- 4 ETHERNET—RJ-45 Ethernet port connects to the Ethernet port on your PC or your home network
- 5 USB—12 Mbps USB port connects to the USB port on your PC
- 6 CABLE—F-Connector connects to an active cable signal from your cable service provider

T10947

DPR2325 Front Panel Description

The front panel of your cable modem gateway provides status lights that indicate how well and at what state your cable modem is operating. After the cable modem gateway is successfully registered on the network, the POWER and CABLE status indicators illuminate continuously to show that the cable modem gateway is active and fully operational. See Front Panel Status Indicator Functions, later in this guide, for more information on front panel status indicator functions.



1. **POWER**—Illuminates solid green to indicate that power is being applied to the cable modem
2. **RECEIVE DATA**—Blinks to indicate that the cable modem is receiving data from the cable network
3. **SEND DATA**—Blinks to indicate that the cable modem is sending data to the cable network
4. **CABLE**—Illuminates solid green when the cable modem is registered on the network and fully operational. This indicator blinks to indicate one of the following conditions:
 - The cable modem is booting up and not ready for data
 - The cable modem is scanning the network and attempting to register
 - The cable modem has lost registration on the network and will continue blinking until it registers again
5. **Ethernet**—Illuminates solid green to indicate that an Ethernet carrier is present and blinks to indicate that data is being transferred on an Ethernet connection to the cable modem
6. **USB**—Illuminates solid green to indicate that a USB carrier is present and blinks to indicate that data is being transferred on a USB connection to the cable modem
7. **PC Wireless**—Illuminates solid green to indicate that a wireless access point is enabled and blinks to indicate that wireless data is being transferred over the wireless connection



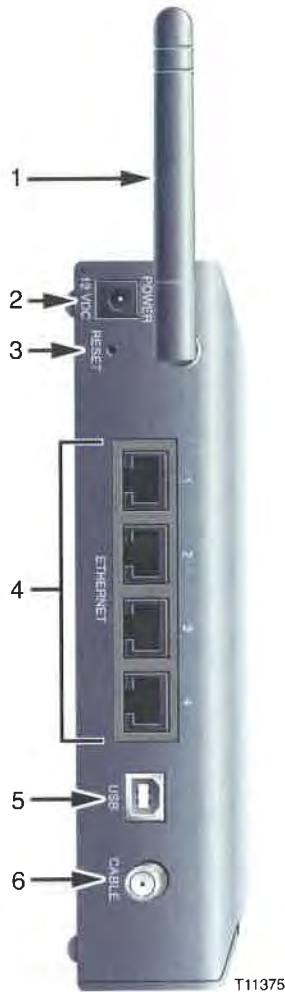
The corresponding LED on the DPR2320 is labeled PC.



After the cable modem gateway is successfully registered on the network, the POWER (LED 1) and CABLE (LED 4) indicators illuminate continuously to indicate that the cable modem gateway is online and fully operational.

DPR2325 Back Panel Description

The following illustration describes the back panel components of the DPR2325.



1. **ANTENNA**—Provides a communication connection for the built-in wireless access point (WAP) to allow wireless devices to communicate with the cable modem
2. **POWER**—Connects the cable modem to the DC output of the AC power adapter that is provided with your cable modem

 **CAUTION:**

Avoid damage to your equipment. Only use the AC power adapter and power cord that is provided with your cable modem.

3. **RESET**—Activating this switch resets the gateway to factory default values and reboots the cable modem



This switch is for maintenance purposes only. Do not use unless directed to do so by your service provider.

4. **ETHERNET**—Four RJ-45 Ethernet ports connect to the Ethernet port on your PC or to an Ethernet hub on your home network
5. **USB**—12 Mbps USB port connects to the USB port on your PC or to a USB hub
6. **CABLE**—F-Connector connects to an active cable signal from your cable service provider

Where is the Best Location for My Cable Modem Gateway?

The ideal location for your cable modem gateway is where it has access to outlets and other devices. Think about the layout of your home or office, and consult with your cable service provider to select the best location for your gateway.

Consider these recommendations:

- Position your PC and cable modem gateway so that they are located near an AC power outlet.
- Position your PC and cable modem gateway so that they are located near an existing cable input connection to eliminate the need for an additional cable outlet. There should be plenty of room to guide the cables away from the modem and the PC without straining or crimping them.
- Airflow around the cable modem gateway should not be restricted.
- Choose a location that protects the cable modem gateway from accidental disturbance or harm.
- Read this user's guide thoroughly before you decide where to place your cable modem gateway.

What are the System Requirements for Internet Service?

To ensure that your cable modem gateway operates efficiently for high-speed Internet service, verify that all of the Internet devices on your system meet or exceed the following minimum hardware and software requirements.



You will also need an active cable input line and an Internet connection.

Minimum System Requirements for a PC

- A PC with a Pentium MMX 133 processor or greater
- 32 MB of RAM
- Web browsing software (Netscape or Internet Explorer)
- CD-ROM drive

Minimum System Requirements for Macintosh

- MAC OS 7.5
- 32 MB of RAM

System Requirements for an Ethernet Connection

- A PC with Microsoft Windows 95 operating system (or later) with TCP/IP protocol installed, or an Apple Macintosh computer with TCP/IP protocol installed
- An active 10/100BaseT Ethernet network interface card (NIC) installed PC

System Requirements for a USB Connection

- A PC with Microsoft Windows 98SE, ME, 2000, or XP operating system
- A master USB port installed in your PC

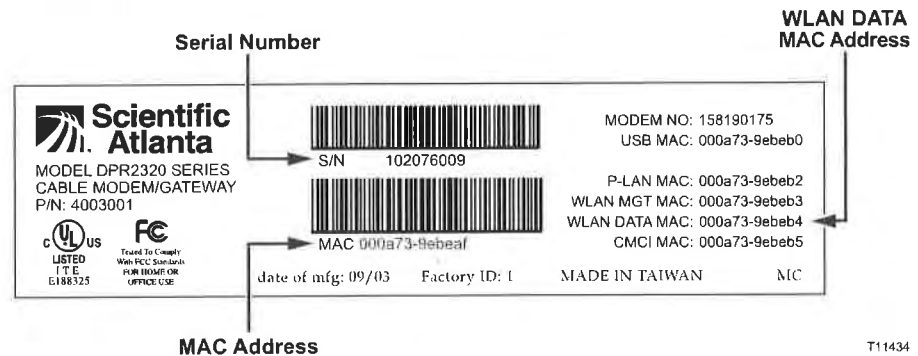
How Do I Set Up My High-Speed Internet Access Account?

Before you can use your cable modem gateway, you need to have a high-speed Internet access account. If you do not have a high-speed Internet access account, you need to set up an account with your local cable service provider. Choose *one* of the following two options.

I Do Not Have a High-Speed Internet Access Account

If you do *not* have a high-speed Internet access account, your cable service provider will set up your account and become your Internet Service Provider (ISP). Internet access enables you to send and receive e-mail, access the World Wide Web, and receive other Internet services. When you contact your cable service provider, they will ask you for the serial number, the Media Access Control (MAC) address, and the WLAN data MAC address of the cable modem.

These numbers appear on a label located on the side of the cable modem gateway. The serial number consists of a series of alphanumeric characters preceded by S/N. The MAC address consists of a series of alphanumeric characters preceded by MAC. The WLAN data MAC address consists of a series of alphanumeric characters preceded by WLAN DATA MAC. See the following illustration of a sample label.



T11434

Write down these numbers in the space provided here.

Serial Number _____
 MAC Address _____
 WLAN DATA MAC Address _____

I Already Have an Existing High-Speed Internet Access Account

If you have an existing high-speed Internet access account, you must give your cable service provider the serial number, the MAC address, and the WLAN data MAC address of the cable modem. Refer to the serial number and MAC address information listed previously in this section.



You may be able to continue to use your existing e-mail account with your cable modem gateway. Contact your cable service provider for more information.

How Do I Connect My Devices to Use the Internet?

You can use your cable modem gateway to access the Internet, and you can share that Internet connection with other Internet devices in your home or office. Sharing one connection among many devices is called networking.

Connecting and Installing Internet Devices

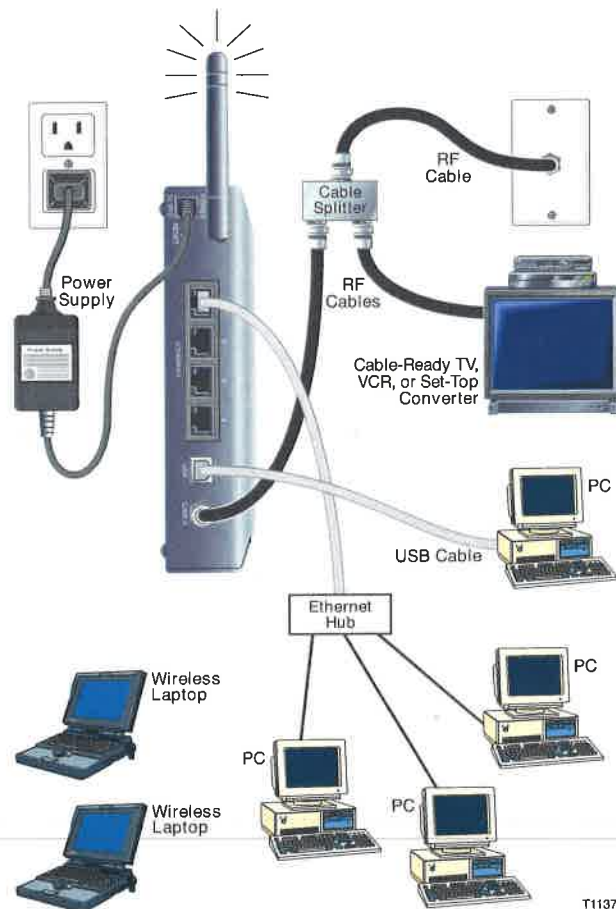
You must connect and install your cable modem gateway to access the Internet. Professional installation may be available. Contact your local cable service provider for further assistance.

To connect devices

The following diagram illustrates one of the various Internet connection options that are available to you. The model shown here is the DPR2325.



The DPR2320 has only one (1) Ethernet port.



T11377

To install the cable modem gateway**WARNING:**

To avoid personal injury or damage to your equipment, follow these steps in the exact order shown.

1. Power down your PC and unplug it from the power source.
2. Connect your PC to *either* the ETHERNET port *or* the USB port using the appropriate data cable. Do not connect your PC to *both* the Ethernet and USB ports at the same time. You *can* connect two separate PCs to the cable modem gateway at the same time by connecting one PC to the Ethernet port and one PC to the USB port.
3. Connect the active RF coaxial cable to the CABLE connector. Use an optional cable signal splitter to add a TV, a DHCT or set-top converter, or a VCR.
4. Insert the AC power adapter cord into the DC POWER connector on the back of the cable modem gateway, and then plug the power adapter into an AC power source.
5. Plug in and power on your networked devices including your PC. The cable modem gateway will then begin an automatic search to locate and sign on to the broadband data network. This process may take up to 5 minutes. The modem will be ready for use when the CABLE indicator on the front panel stops blinking and illuminates continuously.
6. The next step in setting up your cable modem gateway is to configure your Internet devices for Internet access. Choose one of the following options:
 - If you want to use Ethernet connections, you must configure the TCP/IP protocol. To configure the TCP/IP protocol go to How Do I Configure TCP/IP Protocol, next in this guide.
 - If you want to use USB connections, you must install the USB drivers. To install the USB Drivers for USB go to How Do I Install USB Drivers, later in this guide.

How Do I Configure TCP/IP Protocol?

To configure TCP/IP protocol, you need to have an Ethernet Network Interface Card (NIC) with TCP/IP communications protocol installed on your system. TCP/IP is a communications protocol used to access the Internet. This section contains instructions for configuring TCP/IP on your Internet devices to operate with the cable modem gateway in Microsoft Windows or Macintosh environments.

Configuring TCP/IP on Your Internet Devices

TCP/IP protocol in a Microsoft Windows environment is different for each Windows version. Follow the appropriate instructions in this section for your operating system.

To configure Windows 95, 98, 98SE, or ME systems

1. Click Start, select Settings, and choose Control Panel.
2. Double-click the Network icon in the Control Panel window.
3. Read the list of installed network components under the Configuration tab to verify that your PC contains the TCP/IP protocol/Ethernet adapter.
4. Is TCP/IP protocol listed in the installed network components list?
 - If yes, go to step 7.
 - If no, click Add, click Protocol, click Add, and then go to step 5.
5. Click Microsoft in the Manufacturers list.
6. Click TCP/IP in the Network Protocols list, and then click OK.
7. Click the TCP/IP Ethernet Adapter protocol, and then choose Properties.
8. Click the IP Address tab, and then select Obtain an IP address automatically.
9. Click the Gateway tab and verify that these fields are empty. If they are not empty, highlight and delete all information from the fields.
10. Click the DNS Configuration tab, and then select Disable DNS.
11. Click OK.
12. Click OK when the system finishes copying the files, and then close all networking windows.
13. Click YES to restart your computer when the System Settings Change dialog box opens. The computer restarts. The TCP/IP protocol is now configured on your PC and your Ethernet devices are ready for use.
14. Try to access the Internet. If you cannot access the Internet, go to Having Difficulty, later in this guide. If you still cannot access the Internet, contact your cable service provider for further assistance.

EXHIBIT A

How Do I Configure TCP/IP Protocol?

To configure Windows 2000 systems

1. Click Start, select Settings, and choose Network and Dial-up Connections.
2. Double-click the Local Area Connection icon in the Network and Dial-up Connections window.
3. Click Properties in the Local Area Connection Status window.
4. Click Internet Protocol (TCP/IP) in the Local Area Connection Properties window, and then click Properties.
5. Select *both* Obtain an IP address automatically and Obtain DNS server address automatically in the Internet Protocol (TCP/IP) Properties window, and then click OK.
6. Click Yes to restart your computer when the Local Network window opens. The computer restarts. The TCP/IP protocol is now configured on your PC and your Ethernet devices are ready for use.
7. Try to access the Internet. If you cannot access the Internet, go to Having Difficulty, later in this guide. If you still cannot access the Internet, contact your cable service provider for further assistance.

To configure Windows XP systems

1. Click Start, select Connect to, and choose Show all connections.
2. Double-click the Local Area Connection icon in the LAN or High-Speed Internet section of the Network Connections window.
3. Click Properties in the Local Area Connection Status window.
4. Click Internet Protocol (TCP/IP), and then click Properties in the Local Area Connection Properties window.
5. Select *both* Obtain an IP address automatically and Obtain DNS server address automatically in the Internet Protocol (TCP/IP) Properties window, and then click OK.
6. Click Yes to restart your computer when the Local Network window opens. The computer restarts. The TCP/IP protocol is now configured on your PC and your Ethernet devices are ready for use.
7. Try to access the Internet. If you cannot access the Internet, go to Having Difficulty, later in this guide. If you still cannot access the Internet, contact your cable service provider for further assistance.

To configure Macintosh systems

1. Click the Apple icon in the upper left corner of the Finder. Scroll down to Control Panels, and then click TCP/IP.
2. Click Edit on the Finder (gray bar) at the top of the screen. Scroll down to the bottom of the menu, and then click User Mode.
3. Click Advanced in the User Mode window, and then click OK.
4. Click the Up/Down selector arrows located to the right of the Connect Via section of the TCP/IP window, and then click Using DHCP Server.
5. Click Options in the TCP/IP window, and then click Active in the TCP/IP Options window.

Note: In some cases, the Load only when needed option will not appear. If it appears, select the option. A check mark appears in the option.

6. Verify that the Use 802.3 option located in the upper right corner of the TCP/IP window is unchecked. If there is a check mark in the option, deselect the option, and then click Info in the lower left corner.
7. Is there a Hardware Address listed in this window?
 - If yes, click OK. To close the TCP/IP Control Panel window, click File, and then scroll down to click Close. You have completed this procedure.
 - If no, you must power off your Macintosh.
8. With the power off, simultaneously press and hold down the Command (Apple), Option, P, and R keys on your keyboard. Keeping those keys pressed down, power on your Macintosh but do not release these keys until you hear the Apple chime.
9. Continue pressing these keys for at least three chimes, then release the keys and allow the computer to restart.
10. When your computer fully reboots, repeat steps 1 through 7 to verify that all TCP/IP settings are correct. If your computer *still* does not have a Hardware Address, contact your authorized Apple dealer or Apple technical support center for further assistance.

How Do I Install USB Drivers?

To install USB drivers, your PC must be equipped with a USB network interface and a Microsoft Windows 98SE, ME, 2000, or XP operating system. This section contains instructions for installing the USB drivers for the cable modem gateway.



If you are not using the USB interface, skip this section.

Installing USB Drivers

The USB driver installation procedures are different for each operating system. Follow the appropriate instructions in this section for your operating system.

To install Windows 98SE and Windows ME USB drivers

1. Insert the USB Cable Modem Driver Installation Disk into the CD-ROM drive of your PC.
2. Wait until the Power and Cable indicators on the cable modem illuminate solid green.
Result: The Add New Hardware Wizard window opens.
3. Click Next in the Add New Hardware Wizard window.
4. Select Search for the best driver for your device (Recommended) in the Add New Hardware Wizard window, and then click Next.
5. Select CD-ROM drive in the Add New Hardware Wizard window, and then click Next.
6. Select The updated driver (Recommended) in the Add New Hardware Wizard window, and then click Next. □
7. Click Next in the Add New Hardware Wizard window. The Copying Files window opens. After 10 to 20 seconds have passed, the Add New Hardware Wizard window reopens.
8. Click Finish. The USB driver installation is complete.
9. Click Yes in the System Settings Change window to restart your computer. The computer restarts. The USB drivers are now installed on your PC and your USB devices are ready for use.
10. Try to access the Internet. If you cannot access the Internet, go to Having Difficulty, later in this guide. If you still cannot access the Internet, contact your cable service provider for further assistance.

To install Windows 2000 drivers

1. Insert the USB Cable Modem Driver Installation Disk into the CD-ROM drive of your PC.
2. Wait until the Power and Cable indicators on the cable modem illuminate solid green.
3. Click Next in the Found New Hardware Wizard window.
4. Select Search for a suitable driver for my device (recommended) in the Found New Hardware Wizard window, and then click Next.
5. Select CD-ROM drives in the Found New Hardware Wizard window, and then click Next.
6. Click Next in the Found New Hardware Wizard window. The system searches for the driver file for your hardware device.
7. After the system finds the USB driver, the Digital Signature Not Found window opens and displays a confirmation message to continue the installation.
8. Click Yes to continue the installation. The Found New Hardware Wizard window reopens with a message that the installation is complete.
9. Click Finish to close the Found New Hardware Wizard window. The USB drivers are installed on your PC and your USB devices are ready for use.
10. Try to access the Internet. If you cannot access the Internet, go to Having Difficulty, later in this guide. If you still cannot access the Internet, contact your cable service provider for further assistance.

To install Windows XP drivers

1. Insert the USB Cable Modem Driver Installation Disk into the CD-ROM drive of your PC.
2. Wait until the Power and Cable indicators on the cable modem illuminate solid green.
3. Select Install from a list or specific location (Advanced) in the Found New Hardware Wizard window, and then click Next.
4. Select Search removable media (floppy, CD-ROM) in the Found New Hardware Wizard window, and then click Next.
5. Click Continue Anyway in the Hardware Installation window to continue the installation. The Found New Hardware Wizard window reopens with a message that the installation has finished.
6. Click Finish to close the Found New Hardware Wizard window. The USB drivers are installed on your PC and your USB devices are ready for use.
7. Try to access the Internet. If you cannot access the Internet, go to Having Difficulty, later in this guide. If you still cannot access the Internet, contact your cable service provider for further assistance.

How Do I Troubleshoot My Internet Service Installation?

I cannot connect to the Internet

- Verify that the plug to your cable modem gateway AC adapter is properly inserted into an electrical outlet.
- Verify that your cable modem gateway AC adapter is not plugged into an electrical outlet that is controlled by a wall switch. If a wall switch controls the electrical outlet, make sure the switch is in the ON position.
- Verify that the POWER, CABLE, and the appropriate indicator lights for your network connection and on the front panel of your cable modem gateway are illuminated.
- Verify that all cables are properly connected, and that you are using the correct cables.
- Verify that your cable service is active and that it supports two-way service.
- Verify that TCP/IP is properly installed and configured on all devices if you are using the Ethernet connections.
- Verify that you have followed the procedure for Installing the USB Drivers for Windows 98SE, ME, 2000, and XP, earlier in this guide, if you are using the USB connection.
- Verify that you have called your cable service provider and given them the serial number and MAC address of your cable modem gateway.
- If you are using a cable signal splitter so that you can connect the cable signal to other devices, remove the splitter and reconnect the cable so that the cable modem gateway is connected directly to the main cable input. If the cable modem gateway now functions properly, the cable signal splitter may be defective and may need to be replaced.

My cable modem gateway does not register an Ethernet connection

Even new devices do not always have Ethernet capabilities. Verify that your device has a 10/100BaseT Ethernet card and that the Ethernet driver software is properly installed. If you purchase and install an Ethernet card, follow the installation instructions very carefully.

My cable modem gateway does not register a cable connection

- The cable modem gateway works with a standard, 75-ohm, RF coaxial cable. If you are using a different cable, your cable modem gateway will not function properly. Contact your cable service provider to determine if you are using the correct cable.
- You may need to renew the IP address on your PC. Refer to I need to renew the IP address on my PC, next in this section for instructions on how to renew the IP address for your particular operating system.
- Your USB interface may be malfunctioning. Refer to the troubleshooting information in your USB documentation.

I need to renew the IP address on my PC

If your PC cannot access the Internet after the cable modem gateway is online, it is possible that your PC did not renew its IP address. Follow the appropriate instructions in this section for your operating system to renew the IP address on your PC.

To renew the IP Address for Windows 95, 98, 98SE, and ME systems

1. Click Start, and then click Run to open the Run window.
2. Type winipcfg in the Open field, and click OK to execute the winipcfg command. The IP Configuration window opens.
3. Click the down arrow to the right of the top field, and select the Ethernet adapter that is installed on your PC. The IP Configuration window displays the Ethernet adapter information.
4. Click Release, and then click Renew. The IP Configuration window displays a new IP address.
5. Click OK to close the IP Configuration window, you have completed this procedure.



If you cannot access the Internet, contact your cable service provider for further assistance.

To renew the IP Address for Windows 2000, NT, or XP systems

1. Open a Command Prompt (DOS) window.
2. Type ipconfig/release at the C:/ prompt and press Enter. The system releases the IP address.
3. Type ipconfig/renew at the C:/ prompt and press Enter. The system displays a new IP address.
4. Click on the X in the upper-right corner of the window to close the Command Prompt window. You have completed this procedure.



If you cannot access the Internet, contact your cable service provider for further assistance.

What are the Requirements for Ethernet Network Devices?

How Many Ethernet Network Devices Can I Connect?

The WebSTAR Cable Modem Gateways can support several Ethernet network devices using either one of the four Ethernet ports on the back panel of the unit, or using external Ethernet hubs that must be purchased separately. The theoretical maximum number of Ethernet network devices supported by the cable modem gateway is 253. However, under normal circumstances, the number of devices connected should be a much lower number. Contact your cable service provider for more information on the maximum number of Ethernet network devices to connect to the gateway in order to maintain optimal network performance.

What are the Wiring Requirements for Ethernet Networking?

A number of factors can impact the practical limit of the network. Although the WebSTAR Cable Modem Gateway is designed to support several Ethernet network devices, it is important to view the characteristics of the entire network and not just each individual node. The theoretical distance between two 10/100BaseT CAT-5 Ethernet hubs is 382 feet (100 meters). Contact your cable service provider or consult the documentation for your Ethernet network devices for more information.



Scientific-Atlanta recommends that you use CAT-5 Ethernet cables.

Do I Need to Configure the TCP/IP Protocol on My Computer?

In order for you to use Ethernet network devices on your network, you must have the TCP/IP protocol properly configured on your PC. Refer to *How Do I Configure TCP/IP Protocol*, earlier in this guide, for detailed information on configuring the TCP/IP protocol.

How Do I Select and Place Ethernet Network Devices?

You can use a large variety of Ethernet network devices with your cable modem gateway. These include NIC cards, hubs, bridges, etc. Contact your cable service provider or consult the documentation for your Ethernet network devices for more information on configuring Ethernet network devices.

Where is the Best Location for My Ethernet Network Devices?

You should work with your cable service provider to choose the best location for your Ethernet network devices. Consider these recommendations:

- Location of two-way cable outlets
- Distance of the Ethernet network devices from the cable modem gateway
- Location of computers and other equipment from AC power outlets
- Ease of running Ethernet cable to the Ethernet network devices

Now that you have selected a location for your Ethernet network devices, the next step is to place and connect your Ethernet network devices. Go to [How Do I Connect Ethernet Network Devices](#), next in this guide.

How Do I Connect Ethernet Network Devices?

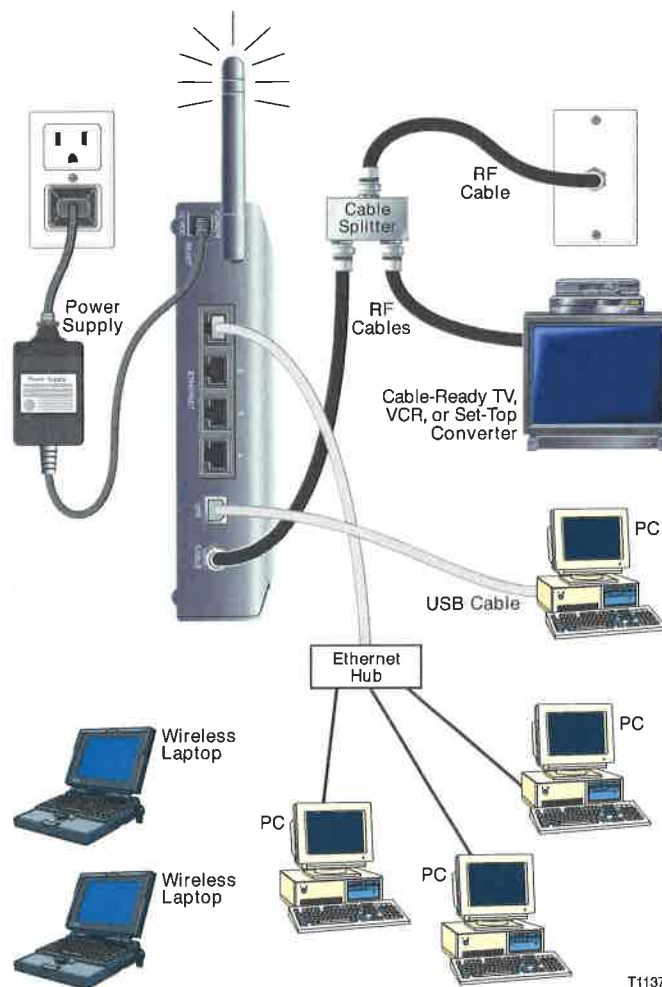
Connecting Ethernet Devices

You must connect your Ethernet devices for use with the cable modem gateway. Professional installation may be available. Contact your local cable service provider for further assistance.

The following diagram illustrates one of the various Ethernet network connection options that are available to you. The model shown here is the DPR2325.




The DPR2320 has only one (1) Ethernet port.



T11377

To connect Ethernet devices

Read the warnings and caution on this page. Then, follow the subsequent installation procedures to ensure proper cable modem gateway operation when connecting Ethernet network devices.

 **WARNING:**

- Hazardous electrical voltages can be present on any connected wiring. Ethernet wiring and connections must be properly insulated to prevent electrical shock. Disconnect power from the cable modem gateway before attempting to connect to any device.
- To avoid personal injury, follow these steps in the exact order shown.

 **CAUTION:**

To prevent possible damage to the equipment, disconnect any other service before connecting your cable modem gateway to other devices.

1. Select locations for Ethernet network devices. For more information, see How Do I Select and Place Ethernet Network Devices, earlier in this guide.
2. Connect an Ethernet port on the cable modem gateway to your PC.
3. Connect additional Ethernet network devices using the other Ethernet ports on the cable modem gateway (DPR2325), or by connecting an Ethernet hub or router to the cable modem gateway.
4. Connect the active RF coaxial cable to the CABLE connector on the back of the cable modem gateway. Use an optional cable signal splitter to add a TV, a DHCT or set-top converter, or a VCR.
5. After all connections are complete, insert the AC power adapter cord into the DC POWER connector on the back of the cable modem gateway, and then plug the power adapter into an AC power source.
6. The cable modem gateway begins an automatic search to locate and sign on to the network. In some unusual circumstances, this process may take up to 5 minutes. The cable modem gateway is ready for use when the CABLE status indicator on the front panel stops blinking and illuminates continuously.
7. Verify that all Ethernet network devices are working properly.



You will not be able to check the Ethernet front panel status indicators on the cable modem gateway until after two or more Ethernet network devices are connected to the cable modem gateway.

What are the Requirements for USB Network Devices?

How Many USB Devices Can I Connect?

Contact your cable service provider for more information on the maximum number of USB network devices to connect to the cable modem gateway in order to maintain optimal network performance.

What are the Wiring Requirements?

Several factors can impact the practical limit of the network. Use correct USB cables. Contact your cable service provider or consult the documentation for your USB network device for more information.

Do I Need to Install USB Drivers on My Computer?

To use USB network devices, you must have the correct USB drivers install on your PC. Refer to How Do I Install USB Drivers, earlier in this guide, for information on installing USB drivers.

How Do I Select and Place USB Network Devices?

You can use a large variety of USB network devices with your cable modem gateway. These include desktop computers, laptop computers, devices with USB ports, USB adapters. Contact your cable service provider or consult the documentation for your USB network devices for more information on selecting USB network devices.

Where is the Best Location for My USB Network Devices?

You should work with your cable service provider to choose the best location for your USB network devices. Consider these recommendations:

- Location of two-way coaxial cable outlets
- Distance of the USB network devices from the cable modem gateway
- Location of computers and other equipment from AC power outlets
- Ease of running USB cable to the USB network devices

Now that you have selected a location for your USB network devices, the next step is to place and connect your USB network devices. Go to *How Do I Connect USB Network Devices*, next in this guide.

How Do I Connect USB Network Devices?

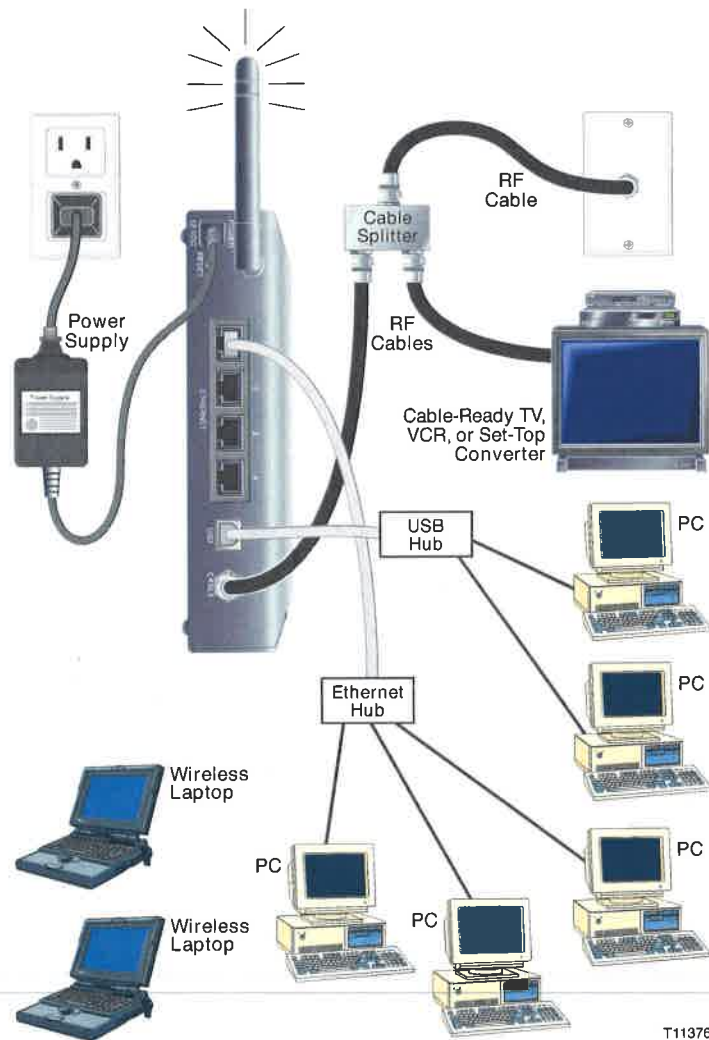
Connecting USB Devices

You must connect your USB devices for use with your cable modem gateway. Professional installation may be available. Contact your local cable service provider for further assistance.

The following diagram illustrates one of the various USB network connection options that are available to you. The model shown here is the DPR2325.




The DPR2320 has only one (1) Ethernet port.



To connect USB devices


Read the warnings and caution on this page. Then, follow the subsequent installation procedures to ensure proper cable modem gateway operation when connecting USB network devices.

 **WARNING:**


- Hazardous electrical voltages can be present on any connected wiring. Ethernet wiring and connections must be properly insulated to prevent electrical shock. Disconnect power from the cable modem gateway before attempting to connect to any device.
- To avoid personal injury, follow these steps in the exact order shown.

 **CAUTION:**

To prevent possible damage to the equipment, disconnect any other service before connecting your cable modem gateway to other devices.


 Verify that you have installed the USB drivers on your PC before continuing with these instructions. See *How Do I Install USB Drivers*, earlier in this guide for more information on installing the USB drivers.

1. Select locations for USB network devices. For more information, see *How Do I Select and Place USB Network Devices*, earlier in this guide.
2. Connect the USB port on the cable modem gateway to your computer.
3. Connect one or more USB network device to the cable modem gateway.

 If you want to connect more than one USB network device to the cable modem gateway or to your computer, you will need to purchase and install a USB hub.

4. Connect the active RF coaxial cable to the CABLE connector on the back of the cable modem gateway. Use an optional cable signal splitter to add a TV, a DHCT or set-top converter, or a VCR.
5. After all connections are complete, insert the AC power adapter cord into the DC POWER connector on the back of the cable modem gateway, and then plug the power adapter into an AC power source.

6. The cable modem gateway begins an automatic search to locate and sign on to the network that provides the telephone service. This process may take up to 5 minutes. The cable modem gateway is ready for use when the CABLE status indicator on the front panel stops blinking and illuminates continuously.
7. Verify that all USB devices are working properly.

 You will not be able to check the USB front panel status indicator on the cable modem gateway until after at least one USB network device is connected and operating on the network.

What are the Requirements for Wireless Network Devices?

How Many Wireless Devices Can I Connect?

The cable modem gateway serves as a wireless access point (WAP). The WAP on the cable modem gateway provides wireless network service to multiple wireless network devices. Contact your cable service provider for more information on the maximum number of wireless network devices to connect to the cable modem gateway in order to maintain optimal network performance.

What are the Requirements for Wireless Networking?

It is important to view the characteristics of the entire network and not just each individual node. The theoretical distance between wireless network devices is 100 feet inside of a building, and 300 feet outdoors.

A number of factors can impact the practical limit of the network. Contact your cable service provider or consult the documentation for your wireless network devices for more information.

How Do I Select and Place Wireless Network Devices?

You can use a large variety of wireless network devices with your cable modem gateway. These include computers, PDAs, etc. On the wireless network, all devices impact the characteristics of the network, because each device transmits a wireless signal. Contact your cable service provider or consult the documentation for your wireless network device for more information on selecting the appropriate wireless network devices for your home or office network.

Where is the Best Location for My Wireless Network Devices?

You should work with your cable service provider to choose the best location for your wireless network devices. Consider these recommendations:

- Distance from the cable modem gateway to the wireless network devices.
- Do not place the cable modem gateway near metallic surfaces that may block the wireless communications path. Wireless communication is "line-of-sight" through non-metallic walls. However, the more structures (walls) the signal must pass through, the weaker the received signal.
- Do not place wireless network devices near a microwave oven. When operating, microwave ovens can interfere with wireless transmissions.
- Do not place your wireless network devices near 2.4 GHz wireless telephones because these telephones may also cause interference with your wireless network.

Now that you have selected a location for your wireless network devices, the next step is to place and install your wireless network devices. Go to How Do I Install Wireless Network Devices, next in this guide.

How Do I Install Wireless Network Devices?

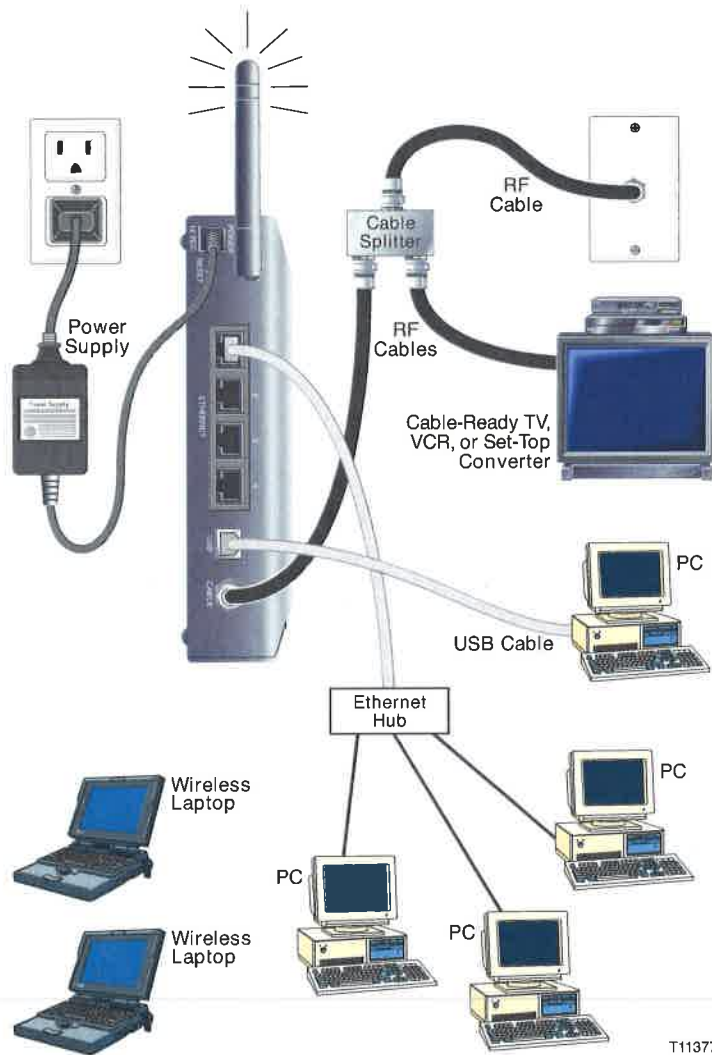
Installing Wireless Network Devices

You must install wireless network devices for use with your cable modem gateway. Professional installation may be available. Contact your local cable service provider for further assistance.

The following diagram illustrates one of the various wireless network connection options that are available to you. The model shown here is the DPR2325.



The DPR2320 has only one (1) Ethernet port.



T11377

To install wireless network devices

Read the warnings and caution on this page. Then, follow the subsequent installation procedures to ensure proper cable modem gateway operation when using wireless network devices.

Follow these steps to install the cable modem gateway for accessing wireless network devices.

**WARNING:**

- Hazardous electrical voltages can be present on any connected wiring. Ethernet wiring and connections must be properly insulated to prevent electrical shock. Disconnect power from the cable modem gateway before attempting to connect to any device.
- To avoid personal injury, follow these steps in the exact order shown.

**CAUTION:**

To prevent possible damage to the equipment, disconnect any other service before connecting your cable modem gateway to other devices.

1. Select locations for wireless network devices. For more information, see *How Do I Select and Place Wireless Network Devices*, earlier in this guide.
2. Connect and install the wireless network device(s).
3. Connect the active RF coaxial cable to the CABLE connector on the back of the cable modem gateway. Use an optional cable signal splitter to add a TV, a DHCT or set-top converter, or a VCR.
4. After all connections are complete, insert the AC power adapter cord into the DC POWER connector on the back of the cable modem gateway, and then plug the power adapter into an AC power source. The cable modem gateway begins an automatic search to locate and sign on to the network that provides the telephone service. In some unusual circumstances, this process may take up to 5 minutes. The cable modem gateway is ready for use when the CABLE status indicator on the front panel stops blinking and illuminates continuously.



Some 2.4 GHz cordless telephones can interfere with wireless signals. Unplug and disconnect any cordless phones until your wireless network is operating properly.

5. Verify that all wireless network devices are working properly.

How Do I Configure the Cable Modem Gateway?

To configure your cable modem gateway, you must access the WebWizard configuration pages. This section provides detailed instructions and procedures for configuring your cable modem gateway to operate correctly and presents an example of each WebWizard page. Use the WebWizard pages to customize your cable modem gateway to your needs rather than using the default settings.

The WebWizard pages and the examples shown in this section are for illustration purposes only. Your pages will differ from the pages shown here.



If you are not familiar with the network configuration procedures detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default settings.

Configuring the Cable Modem Gateway

You must access the WebWizard in order to configure the cable modem gateway. To gain access to the WebWizard, use the Web browser on the PC attached to the cable modem. Type the following IP address and then select Go:
<http://192.168.0.1>

The Web browser accesses the WebWizard and displays the default About Your Modem page. This page displays information about the cable modem gateway.

About Your Modem Page Example

The following illustration is an example of the About Your Modem page.

About Your Modem
 This page provides the basic information about your cable modem

Name	WebSTAR DPR2325
Modem Serial Number	1022060498
Cable Modem MAC Address	00:0A:73:AD:77:C0
Hardware Version	v1.3
Software Version	v2.0.1r1135
Receive Power Level	-47.6 dBmV
Transmit Power Level	8.3 dBmV
Cable Modem Status	Operational

WebSTAR is a trademark of Scientific-Atlanta, Inc. Scientific-Atlanta and the Scientific-Atlanta logo are registered trademarks of Scientific-Atlanta, Inc. ©2004 Scientific-Atlanta, Inc. All rights reserved.

About Your Modem Page Description

The following table provides a description of each field within the About Your Modem page.

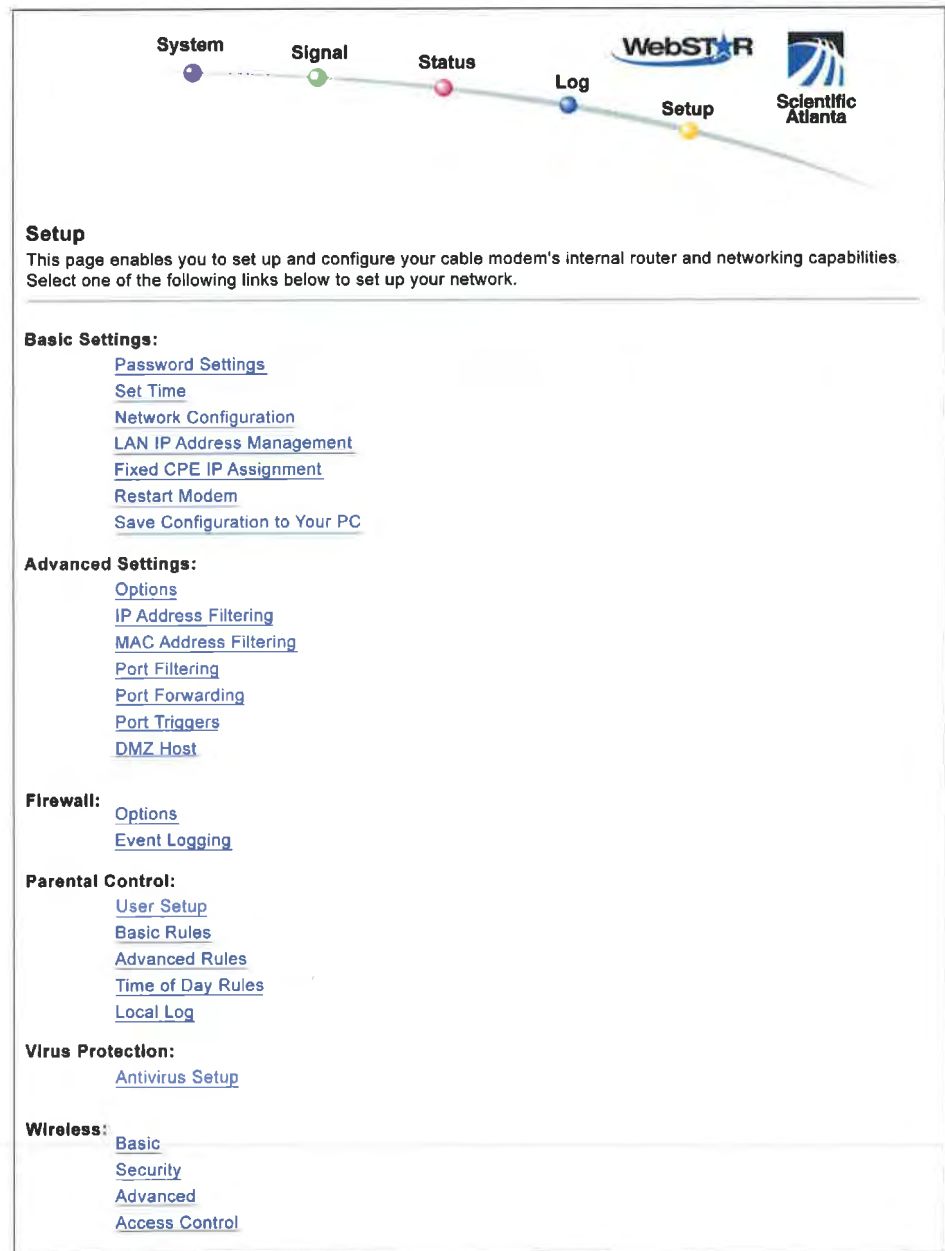
Field Name	Description
Name	The name of the cable modem gateway
Modem Serial Number	A unique sequential series of alphanumeric characters provided to every modem during manufacturing
Cable Modem MAC Address	A unique alphanumeric address for the cable modem coaxial interface, which is used to connect to the cable modem termination system (CMTS) at the headend. A media access control (MAC) address is a hardware address that uniquely identifies each node of a network
Hardware Version	Identifies the revision of the circuit board design
Software Version	Identifies the software version placed into the modem at the time of manufacturing
Receive Power Level	The input level of the downstream CMTS carrier
Transmit Power Level	Indicates the upstream power level
Cable Modem Status	Lists one of the following possible current states of the modem: <ul style="list-style-type: none"> • other • notReady • notSynchronized • phySynchronized • usParametersAcquired • rangingComplete • ipComplete • todEstablished • securityEstablished • psrsmTransferComplete • registrationComplete • operational • accessDenied

Setting Configuration Options

Click Setup on the arc logo located in the upper portion of the About Your Modem screen to access the Setup page. Use the Setup page to access the various configuration options for the cable modem gateway. Detailed descriptions of each configuration option follow later in this guide.

Setup Page Example

The following illustration is an example of the Setup page.



System **Signal** **Status** **Log** **Setup**

WebSTAR
Scientific Atlanta

Setup

This page enables you to set up and configure your cable modem's internal router and networking capabilities. Select one of the following links below to set up your network.

Basic Settings:

- [Password Settings](#)
- [Set Time](#)
- [Network Configuration](#)
- [LAN IP Address Management](#)
- [Fixed CPE IP Assignment](#)
- [Restart Modem](#)
- [Save Configuration to Your PC](#)

Advanced Settings:

- [Options](#)
- [IP Address Filtering](#)
- [MAC Address Filtering](#)
- [Port Filtering](#)
- [Port Forwarding](#)
- [Port Triggers](#)
- [DMZ Host](#)

Firewall:

- [Options](#)
- [Event Logging](#)

Parental Control:

- [User Setup](#)
- [Basic Rules](#)
- [Advanced Rules](#)
- [Time of Day Rules](#)
- [Local Log](#)

Virus Protection:

- [Antivirus Setup](#)

Wireless:

- [Basic](#)
- [Security](#)
- [Advanced](#)
- [Access Control](#)

Setup Page Section Headings

The Setup page is divided into the following section headings:

- Basic Settings
- Advanced Settings
- Firewall
- Parental Control
- Virus Protection
- Wireless

In the Setup page, click the selections listed within these sections to access the WebWizard page for that selection. A description of the selections available in each section follows next.

Basic Settings

The following table provides a description of the pages available from within the Basic Settings section of the Setup page.

Field Name	Description
Password Settings	Use this page to set or modify your password settings
Set Time	Use this page to enable or disable time synchronization by Network Time protocol
Network Configuration	Use this page to enter or modify the basic settings for your network
LAN IP Address Management	Use this page to configure how Internet protocol (IP) addresses are assigned and managed in your network
Fixed CPE IP Assignment	Use this page to reserve IP addresses in the DHCP pool that will be used as static IP addresses in your local network.
Restart Modem	Use this page to restart your cable modem gateway
Save Configuration to your PC	Use this page to save your cable modem RG configuration to your local PC and to restore the RG configuration to your cable modem gateway, if necessary

Advanced Settings

The following table provides a description of the pages available from within the Advanced Settings section of the Setup page.

Field Name	Description
Options	Use this page to enable or disable advanced features on your network
IP Address Filtering	Use this page to configure IP address filters. These filters prevent designated IP addresses from accessing the Internet
MAC Address Filtering	Use this page to configure MAC address filters. These filters prevent designated MAC addresses from accessing the Internet

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Field Name	Description
Port Filtering	Use this page to configure transmission control protocol (TCP) and user datagram protocol (UDP) port filters. These filters prevent a range of TCP/UDP ports from accessing the Internet
Port Forwarding	Use this page to configure port forwarding for local IP addresses. Port forwarding allows you to run a server on the local area network (LAN) by specifying the mapping of TCP/UPD ports to local PCs or to the IP address of other devices. This is a static setting that holds the ports open at all times
Port Triggers	Use this page to configure TCP/UPD port triggers. Port triggering is similar to port forwarding, but is a dynamic function. In other words, the ports are not held open, and the ports close if no outgoing data is detected on the selected ports for a period of 10 minutes
DMZ Host (Demilitarized Zone)	<p>Use this page to configure an IP address that is visible to the wide area network (WAN). DMZ hosting is commonly referred to as "exposed host," and allows you to specify the "default" recipient of WAN traffic that Network Address Translation (NAT) is unable to translate to a known local PC.</p> <p>A DMZ is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. DMZ allows one IP address to be unprotected while others remain protected. The DMZ is located between the Internet and an internal network's line of defense that is a combination of firewalls and bastion hosts.</p> <p>Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and domain name system (DNS) servers</p>

Firewall

The following table provides a description of the pages available from within the Firewall section of the Setup page.

Field Name	Description
Options	Use this page to configure Web page filtering and firewall protection
Event Logging	Use this page to access the firewall event log and to enter your e-mail address in order to receive e-mail alerts related to firewall attacks by hackers

Parental Control

The following table provides a description of the pages available from within the Parental Control section of the Setup page.

Field Name	Description
User Setup	Use this page to add or delete user profiles and to apply access rules to those users
Basic Rules	Use this page to setup access rules that block certain Internet content and certain Web sites
Advanced Rules	Use this page to configure parental control associated with a content rating service
Time of Day Rules	Use this page to configure Web access filters to block all Internet traffic to and from specific network devices based on time of day settings that you select
Local Log	Use this page to view events captured by Parental Control event log feature

Virus Protection

The following table provides a description of the pages available from within the Virus Protection section of the Setup page.

Field Name	Description
Antivirus Setup	Use this page to access a Web site that allows you to download a free evaluation copy of antivirus software

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Wireless

The following table provides a description of the pages available from within the Wireless section of the Setup page.

Field Name	Description
Basic	Use this page to configure your wireless access point (WAP) parameters, including service set identifier (SSID) and channel number
Security	Use this page to configure your WAP authentication and data encryption. Using encryption and authentication prevents unauthorized access to your wireless devices
Advanced	Use this page to configure your WAP data rates and wireless fidelity (WiFi) thresholds
Access Control	Use this page to configure the WAP to restrict access to only selected wireless client devices. Authorized clients are selected by MAC address. Use this page to select Open System or Share Key authentication and to enable and disable broadcast of the WAP SSID

Configuring Your Password Settings

Use the Basic Settings - Password Settings page to set up a password to restrict unauthorized persons from accessing to your cable modem gateway settings. Click Password Settings in the Basic Settings section of the Setup page to access the Password Settings page.



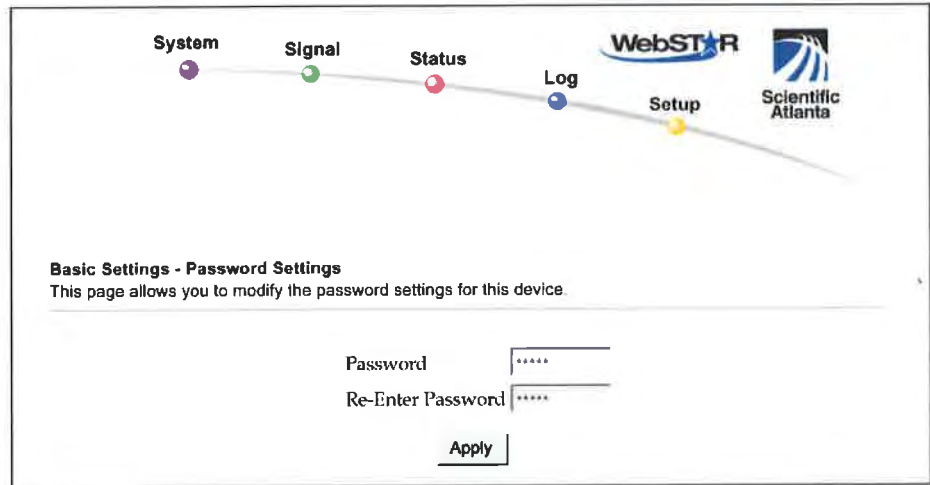
Your gateway modem comes from the factory with no password enabled. We highly recommend that you set up a user password to prevent unauthorized users from modifying the settings of your network.



If you do choose to set up a password, use a password that you can easily remember. Do *not* forget your password.

Setup Basic Settings – Password Settings Page Example

The following illustration is an example of the Basic Settings – Password Settings page.



To set up your password

To set up your password, type your password in the Password field, and then re-type your password in the Re-Enter Password field. Then, click Apply to save your password.



If you set a password, on subsequent access to the WebWizard pages, a screen similar to the following appears. Do *not* forget your password. Write your password and store it in a secure location known only to you.



Configuring Network Time Synchronization

Use the Basic Settings Enable/Disable time synchronization by Network Time protocol page to enable or disable time synchronization by Network Time protocol.



If you are not familiar with the time configuration procedures detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default time synchronization configuration settings.

Click Set Time in the Basic Settings section of the Setup page to access the Basic Settings Enable/Disable time synchronization by Network Time protocol.

Setup Basic Settings – Enable/Disable Time Synchronization by Network Time Protocol Page Example



The following illustration is an example of the Basic Settings Enable/Disable time synchronization by Network Time protocol page.

The screenshot shows a navigation menu at the top with items: System, Signal, Status, Log, and Setup. The 'Setup' item is highlighted. Below the menu, the page title is 'Setup Basic Settings - Enable/Disable Time Synchronization by Network Time Protocol'. The main content area includes the following fields and controls:

- Current System Time: -----:--:--
- Network Time Protocol: Enable Disable
- Latest Update Success: -----:--:--
- Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
- Daylight Savings Time: 60 minutes Enable
- Apply button
- Time Server: [input field] Add Server
- time.nist.gov
- nist1.aol-ca.truetime.com
- nist1-ny.glassey.com
- Remove Server

Setup Basic Settings – Enable/Disable Time Synchronization by Network Time Protocol Page Description

The following table provides a description of the fields within the Basic Settings Enable/Disable time synchronization by Network Time protocol page.

Field Name	Description
Current System Time	Displays the current system time and date
Network Time Protocol	<p>Allows you to enable or disable network time protocol</p>  <p>The gateway will automatically use the time server in your broadband network. Should there be no current time displayed or if the network time is incorrect, enable Network Time Protocol to use a public Internet time server to set the clock in the gateway.</p>
Latest Update Success	Displays the time and date of the last successful time update
Time Zone	Displays the current time zone. The drop-down list allows you to select your local time zone.
Daylight Saving Time	<p>Check the Enable box to adjust the time during periods when Daylight Savings Time is in effect. This setting must be enabled and disabled manually.</p>  <p>If the offset for Daylight Savings Time is other than 60 minutes, enter the offset in the minutes field.</p>
Time Server	When using Network Time Protocol, multiple time servers can be specified for the gateway to query for time of day. The gateway will sequentially step through the listed time servers until it acquires the current time. There are three well known public time servers entered as default servers. You can add and delete time server URLs or IP addresses to and from the list.

Function Keys

Key	Description
Apply	Saves all additions, edits, and changes
Add Server	Allows you to add a network time server
Remove Server	Allows you to remove a network time server

Configuring the Default Network Settings

You can use the default network settings, or, if your system requires different settings to operate correctly, you can change the default network settings using the Setup Basic Settings – Network Configuration page.



If you are not familiar with the network configuration procedures detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default network configuration settings.

Click Network Configuration in the Basic Settings section of the Setup page to access the Setup Basic Settings – Network Configuration page.

Setup Basic Settings – Network Configuration Page Example

The following illustration is an example of the Setup Basic Settings – Network Configuration page.

Setup
Basic Settings - Network Configuration
 This page allows you to enter or modify the basic settings for your network

LAN IP Address	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="0"/> <input type="text" value="1"/>
MAC Address	<input type="text" value="00:0a:73:ad:77:c4"/>
WAN IP Address	<input type="text" value=""/>
Subnet Mask	<input type="text" value=""/>
Gateway IP	<input type="text" value=""/>
Duration	D: -- H: -- M: -- S: --
Expires	<input type="text" value=""/>
<input type="button" value="Renew WAN IP Address Lease"/>	
Host Name	<input type="text" value=""/> (Required by some ISPs)
Domain Name	<input type="text" value=""/> (Required by some ISPs)
Static IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Static IP Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Default Gateway	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Primary DNS (static IP only)	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Secondary DNS (static IP only)	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
<input type="button" value="Apply"/>	

Setup Basic Settings – Network Configuration Page Description

The following table provides a description of the fields within the Setup Basic Settings – Network Configuration page.


Field Name	Description
LAN IP Address	The base IP address of the private home LAN and the WebWizard IP address. Your cable modem gateway assigns private IP addresses to your attached computers by its internal dynamic host configuration protocol (DHCP) server
MAC Address	The MAC address for the WAN. The factory assigned MAC address for the WAN is also referred to as the WLAN Data MAC
WAN IP Address	Display of the public IP address assigned to your gateway by your ISP. The WAN port will be assigned a public IP address automatically by your ISP except when a static IP address is set up as described below. The WAN IP address will be shared by all the PCs in your private local area network to access the Internet
Subnet Mask	Display of the subnet mask for your WAN port. This address is automatically assigned to your WAN port by your ISP except when a static IP address is set up as described later in this table
Gateway IP	Display of the Gateway IP address for your WAN port. This address is automatically assigned to your WAN port by your ISP except when a static IP address is set up as described later in this table
Duration	The length of time your WAN IP address is valid
Expires	The date and time your WAN IP address expires
Host Name	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.
Domain Name	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.
Static IP Address	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.  When setting a static IP address, you must enter the IP address, subnet mask, and default gateway before the static IP address will become operational
Static IP Mask	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Field Name	Description
Default Gateway	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.
Primary DNS	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.
Secondary DNS	This information is usually downloaded to your gateway by your ISP. However, some ISPs require this information to be entered manually. If manual entry is required, your ISP will provide the information for you to enter into this field.

Function Keys

The following function keys appear on the Setup Basic Settings – Network Configuration page.

Key	Description
Renew WAN IP Address Lease	Forces a release and renewal of your WAN IP address
Apply	Saves the values you enter into the fields without closing the screen

Configuring and Managing IP Addresses

Use the Setup Basic Settings – IP Management page to configure how your system manages and assigns IP addresses in your network.



If you are not familiar with the IP management procedures detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default IP management settings.

Click LAN IP Address Management in the Basic Settings section of the Setup page to access the Setup Basic Settings – IP Management page.

Setup Basic Settings – IP Management Page Example

The following illustration is an example of the Setup Basic Settings – IP Management page.

Setup
Basic Settings - IP Management
 This page allows you to configure how IP addresses are assigned and managed in your network.



DHCP Server Yes No
 Starting Local Address 192.168.0.10
 Number of CPEs 50
 Apply

DHCP Client Lease Info				
MAC Address	IP Address	Subnet Mask	Duration	Expires
0050dac4c13f	192.168.0.0.12	255.255.255.000	D:00 H:00 M:00 S:00	-----:--:--

Current System Time: -----:--:--
 Force Available

Setup Basic Settings – IP Management Page Description

The following tables provide a description of the fields within the Setup Basic Settings – IP Management page.

Field Name	Description
DHCP Server	Allows you to enable or disable the DHCP server
Starting Local Address	<p>The starting address used by the built-in DHCP server to distribute Private LAN IP addresses. In the example shown, addresses between 2 and 9 can be used for devices on your Private LAN that require fixed IP addresses such as printers or a device assigned as a DMZ host</p>  <p>The LAN IP address ending in 1 is reserved for the internal gateway server. The LAN IP address ending in 255 is also reserved and should not be used for CPE devices</p>
Number of CPEs	<p>Enter the maximum number of devices allowed to connect to the Private LAN.</p>  <p>The Factory Default is 50. The maximum number of devices is 255. This is the combined total of addresses reserved for static IP addresses, for example, the sum of the IP addresses between 1 and the value entered in the Starting Local Address field and the value entered in the Number of CPEs field.</p> <p>Note: The sum of the value entered in the Starting Local Address field and the value entered in the Number of CPEs field must <i>always</i> be 255 or less.</p>
DHCP Client Lease Info	Displays the MAC address, IP Address, Subnet Mask, Duration and Expiration date of all devices issued an IP address by the built-in DHCP server. This field also displays the current system time and date

Function Keys

The following function keys appear on the Basic Settings – IP Management page.

Key	Description
Apply	Saves the values you enter into the fields without closing the screen
Force Available	Forces the release of an IP address for you to re-use

Reserving IP Addresses

Use the Setup Basic Settings – Fixed CPE IP Assignment page to reserve IP addresses. This feature allows you to assign a fixed IP address to any device in your network by setting static IP addresses in your PC or other network device.

These addresses will be removed from the pool of the IP addresses to be used by your gateway's DHCP server when issuing IP addresses to devices that are connected to your local network.

Reserving IP addresses is useful in making sure that there are no IP address conflicts on the network, for example, two devices using the same IP address. Another example: when using DMZ Host, the IP address for the DMZ Host should always have the same IP address.



If you are not familiar with the Fixed CPE IP Assignment procedures detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default Fixed CPE IP Assignment settings.

Click Fixed CPE IP Assignment in the Basic Settings section of the Setup page to access the Setup Basic Settings – Fixed CPE IP Assignment page.

Setup Basic Settings – Fixed CPE IP Assignment Page Example

The following illustration is an example of the Setup Basic Settings – Fixed CPE IP Assignment page.

System **Signal** **Status** **Log** **Setup**

WebSTAR Scientific Atlanta

Setup
Basic Settings - Fixed CPE IP Assignment
 This page allows you to set fixed IP for LAN CPE devices

MAC Address : : : : : :


Assign to IP : . . .

MAC Address	IP Address	Status
00 0A 73 AD 77 C1 <->	192.168.0.10	Reserved
00 0D 56 12 44 E8 <->	192.168.0.11	Active

Setup Basic Settings – Fixed CPE IP Assignment Page

Description

The following tables provide a description of the fields within the Setup Basic Settings – Fixed CPE IP Assignment page.

Field Name	Description
MAC Address	The MAC address of the PC or device (for example, a printer) for which you want to reserve a specific IP address on the network
Assign to IP	The IP address you assign to the PC or device for which you want to reserve a specific IP address on the network. Only MAC addresses within the range of the gateway's DHCP address pool can be reserved with this feature.  The factory configuration of your gateway sets aside IP addresses 192.168.0.2 through 192.168.0.9 for static IP addresses.

Function Keys

Key	Description
Add Static IP	Adds the Static IP address to the list of assigned IP addresses
Remove Static IP	Removes the Static IP address from the list of assigned IP addresses

Restarting the Gateway Modem

Use the Setup Basic Settings – Restart Cable Modem page to restart your cable modem.

Click Restart Modem in the Basic Settings section of the Setup page to access the Basic Settings – Restart Cable Modem page.

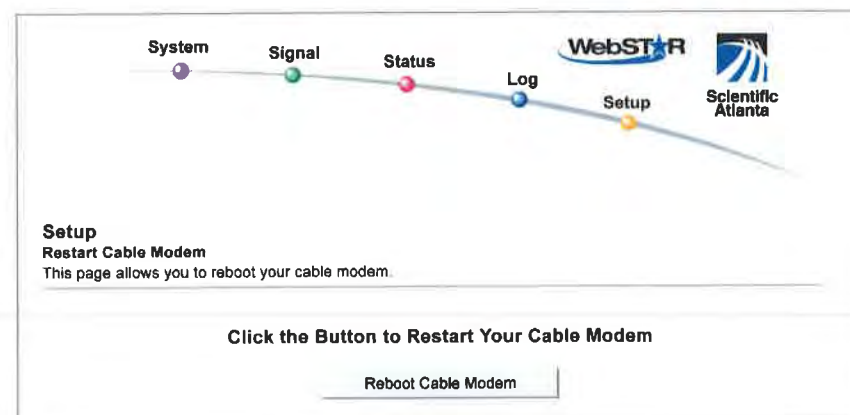
Click Reboot Cable Modem to restart the gateway modem.



Restarting your gateway modem does not reset any of the settings.

Setup Basic Settings - Restart Cable Modem Page Example

The following illustration is an example of the Restart Cable Modem page.



Saving Your Configuration

Use the Setup Basic Settings – Save RG Configuration to Local PC page to save your current cable modem RG configuration to the hard drive on your PC or to a floppy disk. You will then be able to restore the RG configuration, if necessary.

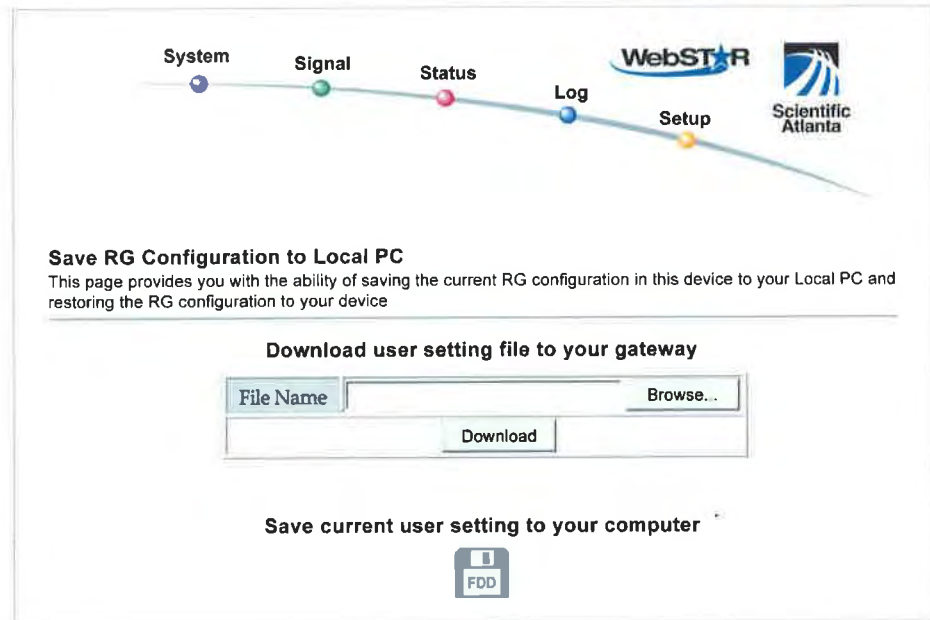


If you are not familiar with the procedures detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default settings.

Click Save Configuration to your PC in the Basic Settings section of the Setup page to access the Setup Basic Settings – Save RG Configuration to Local PC page.

Setup Basic Settings – Save RG Configuration to Local PC Page Example

The following illustration is an example of the Setup Basic Settings – Save RG Configuration to Local PC page.



To Save your current setting to your computer, click the floppy disk icon in the lower portion of the screen. You will be prompted to provide a file name and location for the backup configuration file.

To Restore your setting, click Browse and select the backup configuration file name that you saved on your PC. The path and filename of the backup configuration appears in the File Name field. Then, click Download to restore your configuration file. A Download Success! message appears when the restore is complete.

Enabling and Disabling Advanced Features

Use the Setup Advanced Settings – Options page to enable or disable advanced features on your network. When the wireless interface is disabled, the transmitter is turned off.

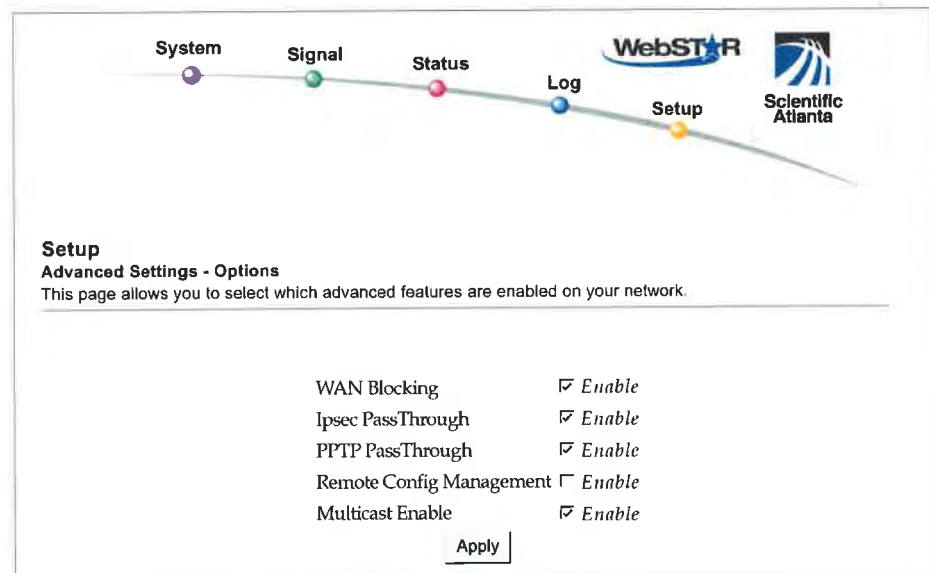


If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced options settings.

Click Options in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – Options page.

Setup Advanced Settings – Options Page Example

The following illustration is an example of the Setup Advanced Settings – Options page.




Setup Advanced Settings – Options Page Description

The following table provides a description of the fields within the Setup Advanced Settings – Options page.



If you make changes in the Setup Advanced Settings – Options page, click Apply to apply and save your new IP address filter settings.

Field Name	Description
WAN Blocking	Checking this box prevents the cable modem gateway from being visible to the WAN. For example, pings to the WAN IP address are not returned
Ipssec PassThrough	Checking this box allows applications that use IPSec (IP Security) to pass through the firewall
PPTP PassThrough	Checking this box allows applications that use Point to Point Tunneling Protocol (PPTP) to pass through the firewall
Remote Config Management	<p>Checking this box enables Remote Configuration Management that allows the user or network operator to view and/or modify the gateway set-up parameters from a location on the WAN, as opposed to the LAN side of the gateway. Access to the set-up parameters is obtained by using the password to access the WebWizard.</p> <p>Enable this feature by checking the Remote Config Management box on the Setup Advanced Settings – Options page. To access your gateway from a remote location, you must also know the WAN IP address of the gateway. To find the WAN IP address, go to the Network Configuration page under Basic Settings. You will find the gateway's WAN IP address list on this page.</p> <p>Enter the WAN IP address of your gateway into the address field of any Web browser using the following format: http://xxx.xxx.xxx.xxx:8080 where xxx.xxx.xxx.xxx represents the WAN IP address of your gateway.</p> <p>Be sure to follow the syntax exactly, and then click Go or press Enter. Your gateway Web pages will appear on the remote computer. You will still need to enter your password to access the Setup pages of your gateway</p> <p> If you choose to enable (check) this feature, be sure to set up a user password to prevent unauthorized access to your gateway settings.</p>
Multicast Enable	Checking this box allows multicasts to pass from the WAN side through to the private network

Configuring IP Address Filters

Use the Setup Advanced Settings – IP Filtering page to configure IP address filters. These filters block a range of IP addresses from accessing the Internet.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced IP filtering settings.

Click IP Address Filtering in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – IP Filtering page.

Setup Advanced Settings – IP Filtering Page Example

The following illustration is an example of the Setup Advanced Settings – IP Filtering page.

Setup
Advanced Settings - IP Filtering
This page allows you to configure IP address filters.

IP Filtering		
Start Address	End Address	Enable
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>
192.168.0.0	192.168.0.0	<input type="checkbox"/>

Apply

Setup Advanced Settings – IP Filtering Page Description

Use this page to specify and enable a range of IP addresses that cannot have access to the Internet. Click Apply to apply and save your new IP address filter settings.

Configuring MAC Address Filters

Use the Setup Advanced Settings – MAC Filtering page to configure MAC address filters. These filters allow you to deny or block access to the Internet by the individual MAC addresses listed in the table. You can also prevent individual PCs from sending outgoing TCP/UDP traffic to the WAN using their MAC address.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced MAC filtering settings.

Click MAC Address Filtering in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – MAC Filtering page.

Setup Advanced Settings – MAC Filtering Page Example

The following illustration is an example of the Setup Advanced Settings – MAC Filtering page.

Setup
Advanced Settings - MAC Filtering
 This page allows you to configure MAC address filters

Block Listed ▾

MAC Address Filters	
MAC 01	00 : 00 : 00 : 00 : 00 : 00
MAC 02	00 : 00 : 00 : 00 : 00 : 00
MAC 03	00 : 00 : 00 : 00 : 00 : 00
MAC 04	00 : 00 : 00 : 00 : 00 : 00
MAC 05	00 : 00 : 00 : 00 : 00 : 00
MAC 06	00 : 00 : 00 : 00 : 00 : 00
MAC 07	00 : 00 : 00 : 00 : 00 : 00
MAC 08	00 : 00 : 00 : 00 : 00 : 00
MAC 09	00 : 00 : 00 : 00 : 00 : 00
MAC 10	00 : 00 : 00 : 00 : 00 : 00
MAC 11	00 : 00 : 00 : 00 : 00 : 00
MAC 12	00 : 00 : 00 : 00 : 00 : 00
MAC 13	00 : 00 : 00 : 00 : 00 : 00
MAC 14	00 : 00 : 00 : 00 : 00 : 00
MAC 15	00 : 00 : 00 : 00 : 00 : 00
MAC 16	00 : 00 : 00 : 00 : 00 : 00
MAC 17	00 : 00 : 00 : 00 : 00 : 00
MAC 18	00 : 00 : 00 : 00 : 00 : 00
MAC 19	00 : 00 : 00 : 00 : 00 : 00
MAC 20	00 : 00 : 00 : 00 : 00 : 00

Apply

Setup Advanced Settings – MAC Filtering Page Description

Use this page to enter the MAC address or MAC addresses of devices whose Internet access you want to control. Click Apply to apply and save your new MAC address filter settings.

Setting Up MAC Address Filters

The Block/Pass drop down menu allows you to block or pass Internet access to the MAC addresses of the devices you list in the MAC Address Filters table. The following table describes the function of the Block/Pass drop down menu.

Field Name	Description
Block Listed (Default)	Select Block to deny Internet access to the MAC addresses of the devices you list in the table. All other MAC addresses will be allowed Internet access.
Pass	Select Pass to allow Internet access only to the MAC addresses of the devices you list in the table. Any MAC addresses <i>not</i> listed in the table will be denied Internet access.

Configuring and Enabling TCP and UDP Port Filters

Use the Setup Advanced Settings – Port Filtering page to configure and enable TCP and UDP port filters. These filters prevent a range of TCP/UDP ports from accessing the Internet. You can also prevent PCs from sending outgoing TCP/UDP traffic to the WAN on specific IP port numbers. This filter is *not* IP address- or MAC address-specific. The system blocks the specified port ranges for *all* PCs.

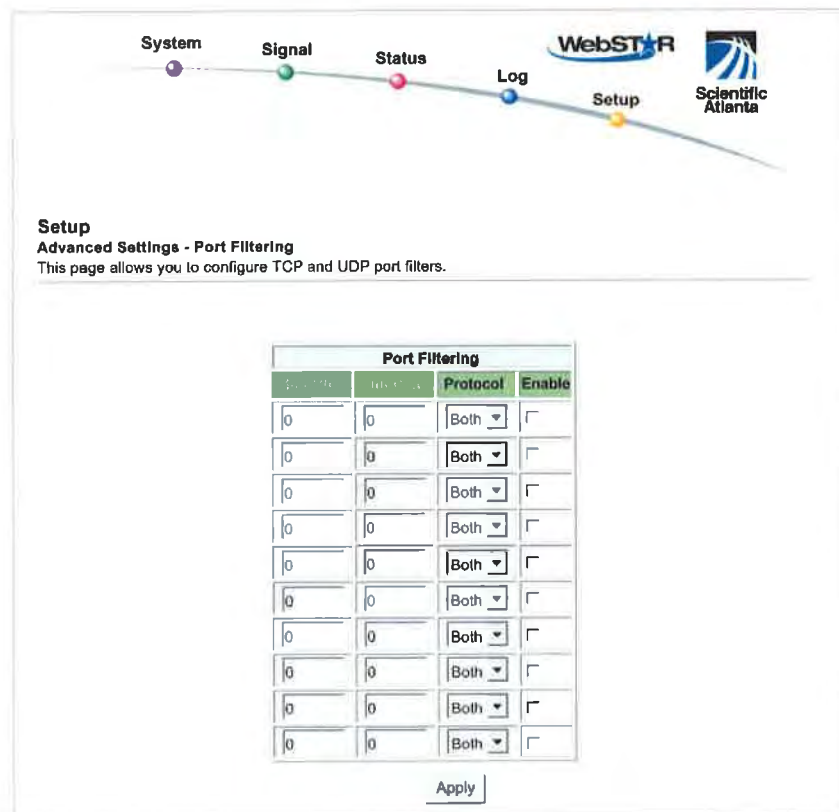


If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced port filtering settings.

Click Port Filtering in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – Port Filtering page.

Setup Advanced Settings – Port Filtering Page Example

The following illustration is an example of the Setup Advanced Settings – Port Filtering page.



Setup Advanced Settings – Port Filtering Page Description

Use this page to enter and enable the desired port filtering ranges and protocols in the appropriate fields and then click Apply to apply and save your new port filtering settings.

Configuring Port Forwarding for Local IP Addresses

Use the Setup Advanced Settings – Port Forwarding page to configure port forwarding for local IP addresses. Port forwarding allows you to run a server on the LAN by specifying the mapping of TCP/UDP ports to a local PC. You must also set up a fixed private LAN IP address for the destination device.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced port forwarding settings.

Click Port Forwarding in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – Port Forwarding page.

Setup Advanced Settings – Port Forwarding Page Example

The following illustration is an example of the Setup Advanced Settings – Port Forwarding page.

The screenshot shows a navigation menu with 'System', 'Signal', 'Status', 'Log', and 'Setup' (highlighted). Below the menu, the page title is 'Setup Advanced Settings - Port Forwarding' with a description: 'This page allows you to configure port forwarding for local IP addresses.' The main content is a table titled 'Port Forwarding' with columns for 'Local IP Addr', 'Start Port', 'End Port', 'Protocol', and 'Enabled'. The table contains 10 rows, each with '192.168.0.0' in the first column, '0' in the second and third columns, 'Both' in the fourth column, and an unchecked checkbox in the fifth column. An 'Apply' button is located at the bottom of the table.

Port Forwarding				
Local IP Addr	Start Port	End Port	Protocol	Enabled
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>
192.168.0.0	0	0	Both	<input type="checkbox"/>

Apply

Setup Advanced Settings – Port Forwarding Page Description

The following example illustrates how to use the port forwarding feature to configure the Microsoft X-Box Online Live for Internet gaming.



For most widely used applications (including Microsoft X-Box Online Live), the WebSTAR firewall automatically maps and opens ports required for that application while the application is in use.

1. Set the device to be used for port forward to a fixed IP address, for example, 192.168.0.5.
2. In the first entry of the Port Forwarding area of the page, enter the same IP address (192.168.0.5) in the Local IP Address field.
3. In the same row, enter the appropriate port numbers in the Start Port and End Port fields.
4. In the same row, select the appropriate protocol from the drop-down list in the Protocol field, and then select the box in the Enable field.
5. To add additional ports, repeat steps 1 through 4, and then go to step 6.
6. Click Apply to apply and save your new port forwarding settings.

Configuring TCP/UDP Port Triggers

Use the Setup Advanced Settings – Port Triggers page to configure TCP/UDP port triggers. Port triggering is similar to port forwarding but is dynamic. In other words, the system does not hold the ports open indefinitely. For example, when the cable modem gateway detects outgoing data on a specific IP port number set in the “Trigger Range,” the resulting ports set in the “Target Range” will open for incoming data. If the system detects no outgoing traffic on the “Trigger Range” ports for a period of 10 minutes, the “Target Range” ports close. This is a safer method for opening specific ports for special applications, such as, video conferencing programs, interactive gaming, and file transfer in chat programs. This is safe because the ports are dynamically triggered and not held open continuously or left open erroneously by the router administrator. Therefore, these ports are not exposed and vulnerable for potential hackers to discover.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced port triggers settings.

Click Port Triggers in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – Port Triggers page.

Setup Advanced Settings – Port Triggers Page Example

The following illustration is an example of the Setup Advanced Settings – Port Triggers page.

Setup
Advanced Settings - Port Triggers
 This page allows you to configure TCP/UDP port triggers.

Port Triggering					
Trigger Range		Target Range		Protocol	Enable
Start Port	End Port	Start Port	End Port		
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>
0	0	0	0	Both	<input type="checkbox"/>

Apply

Setup Advanced Settings – Port Triggers Page Description

Use this page to enter and enable the port forwarding trigger and target range start and end ports along with protocol information in the appropriate fields. The following example illustrates how to use the port triggering feature to configure the Microsoft X-Box Online Live for Internet gaming.



For most widely used applications (including Microsoft X-Box Online Live), the WebSTAR firewall automatically maps and opens ports required for that application while the application is in use.

1. In the first row, enter 88 in *both* Start Port and End Port fields.
2. In the same row, select UDP from the drop-down list in the Protocol field, and then select the box in the Enable field.
3. In the second row, enter 3074 in *both* Start Port and End Port fields.
4. In the same row as the second entry, select Both, and then select the box in the Enable field.
5. Click Apply to apply and save your new port forwarding settings.

Configuring the DMZ Host

Use the Setup Advanced Settings – DMZ Host page to configure an IP address that is visible to the WAN. DMZ hosting is commonly referred to as “exposed host,” and allows you to specify the “default” recipient of WAN traffic that Network Address Translation (NAT) is unable to translate to a known local PC. DMZ allows one IP address to be unprotected while others remain protected.

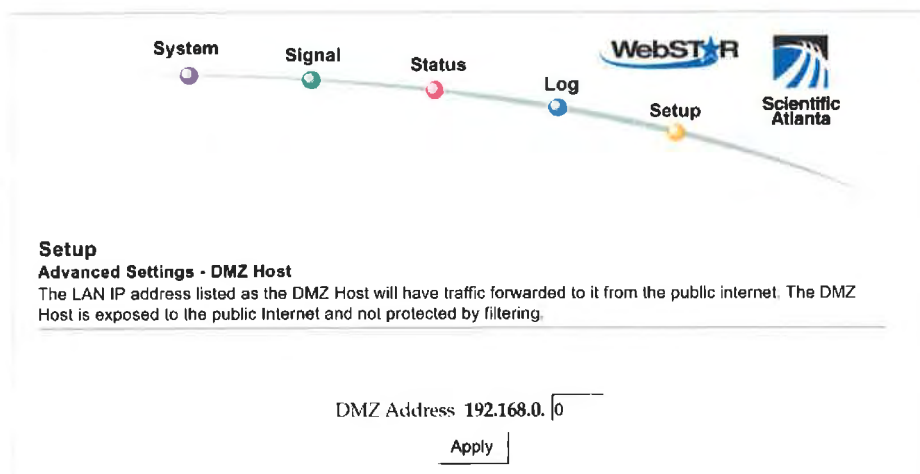


If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default advanced DMZ host settings.

Click DMZ Host in the Advanced Settings section of the Setup page to access the Setup Advanced Settings – DMZ Host page.

Setup Advanced Settings – DMZ Host Page Example

The following illustration is an example of the Setup Advanced Settings – DMZ Host page.



Setup Advanced Settings – DMZ Host Page Description

Use this page to place a Private LAN IP device, for example, an FTP, Mail, or Web server directly on the Internet (bypassing the firewall). You set the server with a fixed IP address as a DMZ Host by entering its IP address in the DMZ Address field. Make sure the IP address used is not in the range of addresses delivered by the built-in DHCP server. After setting up a DMZ Host, all ports on this device are open to the Internet. You may configure only one PC to be the DMZ host. DMZ is generally used for PCs running “problem” applications that use random port numbers and do not function correctly with the specific port triggers or port forwarding setups described earlier in this guide. After entering a DMZ Address, click Apply to apply and save your new DMZ Host setting.

Configuring Firewall Protection

Use the Setup Firewall – Options page to configure Web page filtering and firewall protection. This page allows you to enable various firewall protection filters.

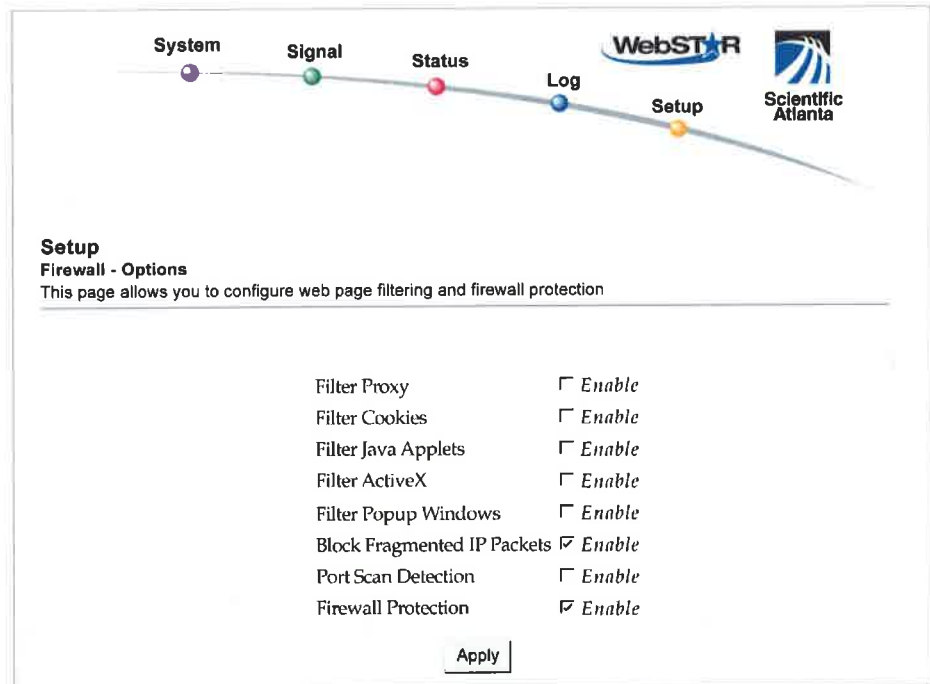


If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default firewall options settings.

Click Options in the Firewall section of the Setup page to access the Setup Firewall – Options page.

Setup Firewall – Options Page Example

The following illustration is an example of the Setup Firewall – Options page.



Setup Firewall – Options Page Description

This section describes the section headings and fields descriptions of the Setup Firewall – Options page.



If you make changes in *any* of the fields in the Setup Firewall – Options page, click Apply to apply and save your Firewall settings.

Content Filtering

The following table provides a description of each field name within the Setup Firewall – Options page.

Field Name	Description
Filter Proxy	Enables/disables proxy
Filter Cookies	Enables/disables cookie blocking. This feature filters the unsolicited delivery of cookies to devices from the Internet to devices in your private local network. Cookies are computer files that contain personal information or Web surfing behavior data.
Filter Java Applets	Enables/disables java applets. This feature helps to protect the devices in your private network from irritating or malicious Java applets that are sent, unsolicited, to devices in your private network from the Internet. These applets run automatically when they are received by a PC.
Filter ActiveX	Enables/disables ActiveX controls. This feature helps to protect the devices in your private network from irritating or malicious ActiveX controls that are sent, unsolicited, to devices in your private network from the Internet. These ActiveX controls run automatically when they are received by a PC.
Filter Popup Windows	Enables/disables popup windows. Some commonly used applications employ popup windows as part of the application. If you disable popup windows, it may interfere with some of these applications.
Block Fragmented IP Packets	Enables/disables filtering of fragmented IP packets. This feature helps protect your private local network from Internet based denial of service attacks.
Port Scan Detection	Enables/disables the gateway from responding to Internet based port scans. This feature is designed to protect your private local network from Internet based hackers who attempt to gain unsolicited access your network by detecting open IP ports on your gateway.
Firewall Protection	Enables/disables the firewall. When the firewall is enabled, the firewall will allow most commonly used applications to automatically open IP ports and pass data without any special setup or manual port configuration.

Configuring Firewall Event Logging and E-mail Alerts

Use the Setup Firewall – Event Logging page to access the firewall event log and allows you to enter your e-mail address in order for you to receive e-mail alerts related to firewall attacks by hackers.



If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default firewall event logging settings.

Click Event Logging in the Firewall section of the Setup page to access the Setup Firewall – Event Logging page.

Setup Firewall – Event Logging Page Example

The following illustration is an example of the Setup Firewall – Event Logging page.

Setup
Firewall - Event Logging
This page provides access to the firewall event log and allows you to enter your email address for email alerts related to firewall attacks.

Enable Email Address
SMTP Server Name
Email Alerts Enable

Description	Count	Last Occurrence	Target	Source
-------------	-------	-----------------	--------	--------

Setup Firewall – Event Logging Page Description

The Setup Firewall – Event Logging page shows events captured by the firewall. The log displays the following items:

- Description of the event
- Number of events that have occurred
- Last occurrence of an event
- Target and source addresses

You can configure the system to e-mail log events to the administrator in order for the administrator to monitor the firewall.

This section describes the section headings and fields descriptions of the Setup Firewall – Event Logging page.

Field Name	Description
Enable Email Address	Allows you to enter the e-mail address of the person who monitors the firewall. When an event occurs, it will be logged and an email will be sent to this address automatically reporting the event.
SMTP Server Name	Allows you to enter the mail server name of your outgoing mail server, or the mail server of your Internet service provider (ISP)
E-mail Alerts	Allows you to enable or disable sending e-mail alerts
Description	Describes what event was detected by the gateway's firewall
Count	Displays the number of times the event has been detected
Last Occurrence	Displays the time the last occurrence of this event was detected
Target	Displays the IP address of the device in your private local network to which the event was directed along with the IP port number targeted by the event
Source	Displays the IP address of the Internet based source of the event along with the IP port number used by that device

Function Keys

The following function keys appear on the Setup Firewall – Event Logging page.

Key	Description
Apply	Saves the values you enter into the fields without closing the screen
E-mail Log	Allows you to force the system to send an e-mail alert even if the E-mail Alerts box is left unchecked
Clear Log	Allows you to clear all entries in the log

Configuring Parental Control

Use the Setup Parental Control – User Setup page to configure parental controls on the cable modem gateway, and to add or delete the individuals who are authorized to set parental controls.



If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default parental control settings.

Click User Setup in the Parental Control section of the Setup page to access the Setup Parental Control – User Setup page.

Setup Parental Control – User Setup Page Example

The following illustration is an example of the Setup Parental Control – User Setup page.

System Signal Status Log Setup

WebSTAR Scientific Atlanta

User Configuration

Add User

User Settings

1. Default Enable Remove User

Password: _____

Re-Enter Password: _____

Trusted User: Enable

Content Rule: _____

Time Access Rule: _____

Available Rules: [Icon] Current Used Rules (Max: 4): [Remove]

Session Duration: 1440 min

Inactivity time: 0 min

Apply

Setup Parental Control – User Setup Page Description


This section describes the section headings and fields descriptions of the Setup Parental Control – User Setup page. This page allows you to set up user profiles. Each profile can be assigned customized levels of Internet access as defined by the access rules assigned to that user’s profile.






Once you define and enable user profiles, each user must sign-on each time they wish to access the Internet. The user can sign-on when the pop-up sign-on screen appears in their Web browser. The user must enter their correct user name and password in order to gain Internet access.

Important:

- Make sure to disable pop-up blockers on your Web browser when using user profiles.
- User names and passwords are case-sensitive.

Field Name	Description
Add User	Allows you to add a new user profile. Enter the name of the user and click the Add User button to add the user to the list.
User Settings	<p>Allows you to edit a user profile by using the drop-down menu to edit a user profile. The drop-down menu allows you to recall the profile to be edited. User names and passwords are case-sensitive.</p> <p>Make sure to check the Enable box to activate the user profile. If a profile is not active, that user will not have any access to the Internet.</p> <p>To remove a user profile, use the drop-down menu to select the user to be removed and click the Remove User button.</p>
Password	<p>Enter the selected user’s password in this field. Each user must enter their User Name and Password each time they use the Internet. User names and passwords are case-sensitive.</p> <p> The Gateway will allow each user access to the Internet, subject to the rules selected on this page for that user.</p>
Re-Enter Password	Re-enter the same password for confirmation of the password in the previous field.
Trusted User	Check this box if the currently selected user is to be designated a trusted user. Trusted users are not subject to Internet access rules.

Field Name	Description
Content Rule	Select the Content Rule for the current user profile. Content Rules must first be defined by going to the Rules Configuration page. You can access the Rule Configuration page by clicking on the " <u>Basic Rules</u> " link under the Parental Control section of the Setup page.
Time Access Rule	Select the Time Access Rule for the current user profile. Time Access Rules must first be defined by going to the Time of Day Filter page. You can access the Time of Day Filter page by clicking on the " <u>Time of Day Rules</u> " link under the Parental Control section of the Setup page.
Session Duration	1440 minutes (factory default). Enter the amount of time in minutes that the user will be granted Internet access beginning at the time they sign on using their User Name and Password.  Set the Session Duration to 0 (zero) to prevent session timeout.
Inactivity time	60 minutes (factory default). Enter the amount of time during a user session where there is no Internet access activity, indicating that the user is no longer online. If the inactivity timer is triggered, the user session will be closed automatically. In order to regain Internet access, the user must log in again with their User Name and Password.  Set the Inactivity time value to 0 (zero) to prevent timeout due to inactivity.
Available Rules	Lists available rules. Apply a rule by selecting it from the list and adding it to the current user profile.  Create rules using the Parental Control Setup pages that follow next.
Current Used Rules	Lists rules in use for the current user profile. You can apply a maximum of four rules to each user profile.

Function Keys

The following function keys appear on the Setup Parental Control – User Setup page.

Key	Description
Add User	Adds and saves a new user to the list of user profiles
Remove User	Removes the selected user from the list of user profiles
Apply	Saves all additions, edits, and changes

Configuring Parental Controls Basic Rules

Use the Setup Parental Control – Basic Setup page to select the rules that block certain Internet content and certain Web sites.



If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default parental control settings.

Click Basic Rules in the Parental Control section of the Setup page to access the Setup Parental Control – Basic Setup page.

Setup Parental Control – Basic Setup Page Example

The following illustration is an example of the Setup Parental Control – Basic Setup page.

Setup
Parental Control - Basic Setup
This page allows basic selection of rules which block certain Internet content and certain Web sites. When you change your Parental Control settings, you must click on the appropriate "Apply", "Add" or "Remove" button for your new settings to take effect. If you refresh your browser's display, you will see the currently active settings.

Rule Configuration
Add Rule

Rule Settings
No rules entered Remove Rule

Keyword List **Blocked Domain List** **Allowed Domain List**

Add Keyword Add Domain Add Allowed Domain
Remove Keyword Remove Domain Remove Allowed Domain

Override Password
If you encounter a blocked website, you can override the block by entering the following password

Password
Re-Enter Password
Access Duration 30
Apply

Setup Parental Control – Basic Setup Page Description

This section describes the section headings and fields descriptions of the Setup Parental Control – Basic Setup page. This page allows you to create Internet access rules based on the content found in the URLs of Internet sites.


Field Name	Description
Rule Configuration	<p>Allows you to add a new content rule. Enter the name of the rule and click the Add Rule button to add the content rule to the list. Content rules are used to restrict Internet access based on IP addresses, domains, and keywords found in the URLs of Internet sites.</p>  <p>It may be useful to set up your first rule as "No Rule," without any restrictions or settings. This setting will allow you to assign "No Rule" status to users who are not subject to "content-related" access restrictions.</p>
Rule Settings	<p>Allows you to edit a content rule by using the drop-down menu to recall the rule to be edited.</p> <p>To remove a user profile, use the drop-down menu to select the rule to be removed and click on the Remove Rule button.</p>
Keyword List	<p>Allows you to create a list of keywords. Any attempt to access a URL that contains any of the keywords in this list will be blocked by the gateway.</p>
Blocked Domain List	<p>Allows to create a list of Domains that the gateway should block access to. Any attempt to access any of the Domains in this list will be blocked by the gateway.</p>
Allowed Domain List	<p>Allows you to create a list of Domains to which the gateway allows access.</p>
Override Password	<p>Allows you to create a password to temporarily override user access restrictions to a blocked Internet site.</p>
Re-enter Password	<p>Reenter the same password for confirmation of the override password in the previous field.</p>
Duration	<p>Allows you to designate an amount of time in minutes that the Override password will allow temporary access to a restricted Internet site.</p>

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Function Keys

The following function keys appear on the Setup Parental Control – Basic Setup page.

Key	Description
Add Rule	Adds and saves a new Rule to the list of content Rules
Remove Rule	Removes the selected rule from the content rule list
Add/Remove Keyword	Allows you to add new keywords to the list or to delete selected keywords from the list
Add/Remove Domain	Allows you to add new domains to the list or to delete selected domains from the list
Add/Remove Allowed Domain	Allows you to add new domains to the list or to delete selected domains from the list
Apply	Saves all additions, edits, and changes

To use keyword and domain blocking

Keyword and Domain blocking allows you to restrict access to Internet sites by blocking access to those sites based on a word or a text string contained in the URLs used to access those Internet sites.

Domain blocking allows you to restrict access to Web sites based on the site's Domain Name. The Domain Name is the portion of the URL that precedes the familiar .COM, .ORG, or .GOV extension.

Keyword blocking allows you to block access to Internet sites based on a Keyword or text string being present anywhere in the URL, not just in the Domain Name.




The Domain blocking feature blocks access to any Domain in the Domain List. It will also block Domains, any portion of which contains an exact match to entries in the list.

For example, if you enter example.com as a Domain, any site that contains "example.com" will be blocked. Generally, you do not want to include "www." in a Domain Name since doing so limits the blocking to only the site that matches that Domain Name exactly. For instance, if you enter www.example.com into the list, only the one site that matches that name exactly will be blocked. Consequently, if you do not include the "www.," then all sites within and associated with "example.com" will be blocked.

Configuring Parental Control Advanced Settings

Use the Setup Parental Control – Advanced Settings page to configure parental control rules that apply to the home network.

 If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default parental control settings.

Click Advanced Rules in the Parental Control section of the Setup page to access the Setup Parental Control – Advanced Settings page.

Setup Parental Control – Advanced Settings Page Example


The following illustration is an example of the Setup Parental Control – Advanced Settings page.



Setup
Parental Control - Advanced Settings
 This page allows configuration of parental control rules that apply to the home network.

Ratings Service	
Subscription Status :	Active
Expiration Date :	WED DEC 31 13:53:32 2003

Rule Settings
 No rules entered.

Categories  CERBERTAH			
<input type="checkbox"/> Abortion	<input type="checkbox"/> Alcohol	<input type="checkbox"/> Criminal Skills	<input type="checkbox"/> Cult
<input type="checkbox"/> Drugs	<input type="checkbox"/> Finance and Investing	<input type="checkbox"/> Gambling	<input type="checkbox"/> Glamour
<input type="checkbox"/> Hacking	<input type="checkbox"/> Hate	<input type="checkbox"/> Hate Site	<input type="checkbox"/> Hate Speech
<input type="checkbox"/> Job Search	<input type="checkbox"/> Lingerie	<input type="checkbox"/> Mature Content	<input type="checkbox"/> News
<input type="checkbox"/> Nudism and Naurism	<input type="checkbox"/> Occult	<input type="checkbox"/> Personals and Dating	<input type="checkbox"/> Pornography
<input type="checkbox"/> Sexual Advice	<input type="checkbox"/> Sexual Education	<input type="checkbox"/> Sexual Orientation	<input type="checkbox"/> Shopping
<input type="checkbox"/> Sports	<input type="checkbox"/> Tobacco	<input type="checkbox"/> Travel	<input type="checkbox"/> Violence
<input type="checkbox"/> Weapons			

[Clear All](#) [Check All](#)

Setup Parental Control - Advanced Settings Page Description

This section describes the section headings and fields descriptions of the Setup Parental Control – Advanced Settings page.



A subscription is required. You must subscribe to the Parental Control Service by clicking on the link displayed on the Setup Parental Control Advanced Settings page.

Field Name	Description
Ratings Service	Your Internet Service provider may offer advanced parental control services. Advanced parental control utilizes Internet based servers to rate Web sites for undesirable content. The rating service will evaluate and rate every Internet site that a user attempts to access through your gateway. The process is extremely fast and does not affect the time it takes to bring up Internet sites on your browser. If a category (or categories) is selected from the rating service category list, then access to any Internet site that has a rating that matches the selected category will be blocked by the gateway.
Subscription Status	Active – Subscription to a rating service is active. Inactive (factory default) – No rating service available.
Rules Settings	This field allows you to attach the selected rating service categories to a previously defined parental control access rule. Use the Rule Setting drop down menu to select the rule to which you want to apply the current set of selected categories.

Configuring Parental Control Time of Day Access Filters

Use the Setup Parental Control – Time of Day Access Filter page to configure Web access filters to block all Internet traffic to and from specific network devices based on day of week and time of day settings that you select.



If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default parental control settings.

Click Time of Day Rules in the Parental Control section of the Setup page to access the Parental Control – Time of Day Access Filter page.

Setup Parental Control – Time of Day Access Filter Page Example

The following illustration is an example of the Setup Parental Control – Time of Day Access Filter page.



The cable modem gateway uses the network time of day clock that is managed by your data service provider. The time of day clock must be accurate and represent the time of day in your time zone for this feature to operate properly. Verify that the Status and Set Time pages reflect the correct time of day. If they do not reflect the correct time of day, contact your data service provider. You can also adjust your settings to account for the difference.

Function Keys

The following function keys appear on the Setup Parental Control – Time of Day Access Filter page.

Key	Description
Add	Allows you to add a new Time of Day access filter or rule. Enter the name of the filter and click the Add key to add the filter to the list. Time of Day rules are used to restrict Internet access based on the day and time.
Remove	Removes the selected filter from the Time of Day filter list.
Apply	Saves all additions, edits, and changes.

Configure Parental Control Event Reporting

Use the Setup Parental Control – Event Log page to view events captured by the parental control event-reporting feature.

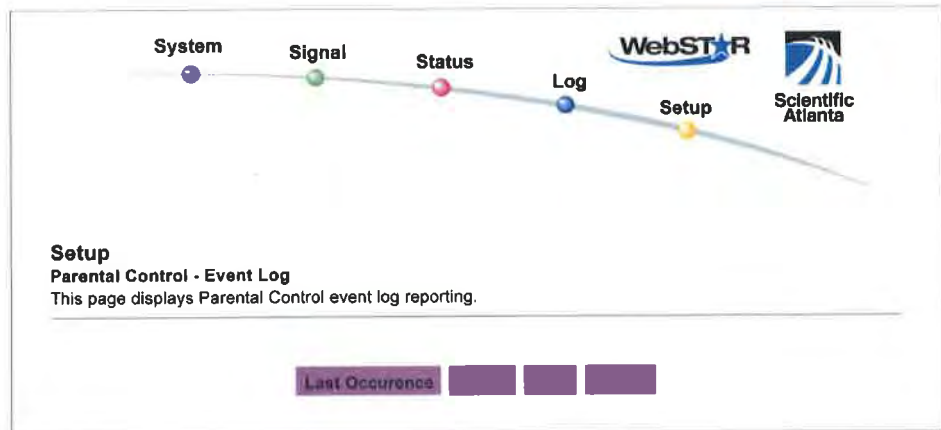


If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default parental control settings.

Click Local Log in the Parental Control section of the Setup page to access the Setup Parental Control – Event Log page.

Setup Parental Control – Event Log Page Example

The following illustration is an example of the Setup Parental Control – Event Log page.



Setup Parental Control – Event Log Page Description

This section describes the section headings and fields descriptions of the Setup Parental Control – Event Log page. This page allows you to track, by user, any attempts made by that user to access Internet sites that are restricted.

Field Name	Description
Last Occurrence	Displays the time of the most recent attempt to access a restricted Internet site
Target	Displays the URL of the restricted site
User	Displays the user who attempted a restricted site
Source	Displays the IP address of the PC which was used when attempting to access a restricted Web site

Configuring Virus Protection

Use the Setup Virus Protection – Antivirus Setup page to access a Web site that allows you to download a free evaluation copy of antivirus software.

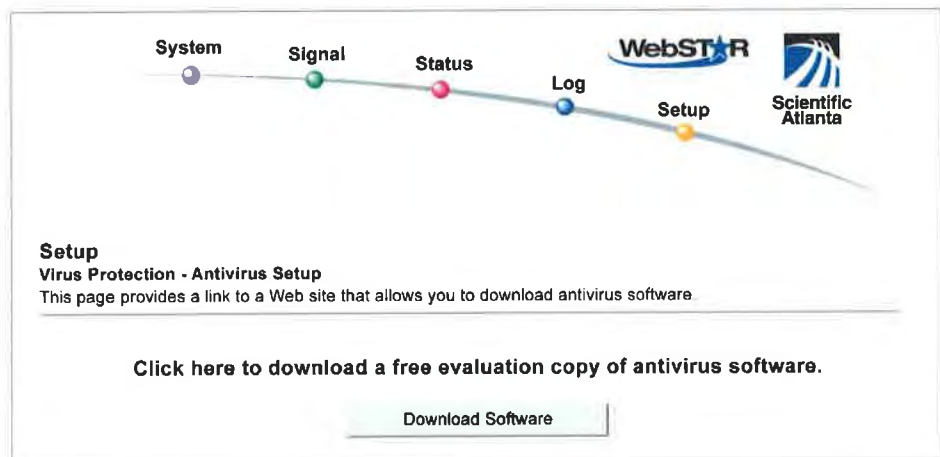


If you are not familiar with the settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default antivirus settings.

Click Antivirus Setup in the Virus Protection section of the Setup page to access the Setup Virus Protection – Antivirus Setup page.

Setup Virus Protection – Antivirus Setup Page Example

The following illustration is an example of the Setup Virus Protection – Antivirus Setup page.



Function Keys

The following function key appears on the Setup Virus Protection – Antivirus Setup page.

Key	Description
Download Software	Click to download a free evaluation copy of antivirus software.

Configuring Your Wireless Access Point Parameters

Use the Setup Wireless – Basic page to configure your wireless access point (WAP) parameters, included SSID and channel number.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default wireless basic settings.

Click Basic in the Wireless section of the Setup page to access the Setup Wireless – Basic page.

Setup Wireless – Basic Page Example

The following illustration is an example of the Setup Wireless – Basic page showing the factory default settings.

The screenshot shows a navigation menu at the top with buttons for System, Signal, Status, Log, and Setup. The Setup button is highlighted. The page title is "WebSTAR Scientific Atlanta". Below the navigation is the heading "Wireless - Basic" and a description: "This page allows you to configure your wireless access point parameters, including SSID and channel number." The configuration fields are as follows:

Access Point:	Enabled
Service Set Identifier (SSID)	WebSTAR
Basic Service Set Identifier (BSSID)	00:0A:73:AD:77:C0
Country:	USA
New Channel:	1
Current Channel:	1
Encryption Mode:	128-Bit Encryption




An "Apply" button is located at the bottom right of the configuration area.

Setup Wireless – Basic Page Description

This section describes the section headings and fields descriptions of the Setup Wireless – Basic page.



If you make changes in the Setup Wireless – Basic page, click Apply to apply and save your wireless basic settings.

Field Name	Description
Access Point	Allows you to turn the access point on the gateway on or off
Service Set Identifier (SSID)	The name assigned to this access point  The factory default for the SSID field should contain the product name WebSTAR.
Basic Service Set Identifier (BSSID)	The MAC address of the access point
Country	Allows you to select the country in which you are using your access point
New Channel (1-11)	Allows setting a communications channel for your access point  Wireless networking channels overlap. Channels 1, 6, and 11 do not overlap with each other. For best performance, select one of these channels. If there are other access points in use in the area, select one of these channels that is farthest away from the other access points. Example: If channel 8 is in use by another access point, use channel 1 for your wireless network.  If your wireless network is not operating correctly, or if external devices are interfering with your signal, select a different channel. Use your PC wireless utility software to scan for other access points in your area.
Current Channel	Present channel the WAP is using
Encryption Mode	Shows current encryption mode

Configuring Your Wireless Network Privacy and Encryption Parameters

Use the Setup Wireless – Privacy page to configure your WAP wired equivalent privacy (WEP) encryption keys and authentication.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default wireless privacy settings.

Click Security in the Wireless section of the Setup page to access the Setup Wireless – Privacy page.

Important: Your WebSTAR Cable Modem Gateway ships from the factory with 128-bit WEP encryption enabled to provide you with a *basic* level of wireless network security. To gain initial access to your wireless network, select 128-bit WEP encryption on your computer's wireless adapter and enter the 128-bit encryption key to match the key setup in your gateway. The factory default 128-bit key in the gateway is 26 zeros (see the following example). You can continue to use this factory default key. However, to maximize your wireless security, it is highly recommended that you use something other than the factory default key.

Setup Wireless – Privacy Page Example

The following illustration is an example of the Setup Wireless – Privacy page.

Setup
Wireless - Privacy
 This page allows you to configure your wireless access point WEP encryption keys and authentication

Network Authentication: Disabled

WPA Pre-Shared Key: _____

WPA Group Rekey Interval: 0

RADIUS Server: 0000

RADIUS Port: 1812

RADIUS Key: _____

Data Encryption: WEP (128-bit)

Shared Key Authentication: Optional

PassPhrase: _____ **Generate WEP Keys**

64 bits Key 1: _____

64 bits Key 2: _____

64 bits Key 3: _____

64 bits Key 4: _____

128 bits Key 1: 00000000000000000000000000000000

128 bits Key 2: 00000000000000000000000000000000

128 bits Key 3: 00000000000000000000000000000000

128 bits Key 4: 00000000000000000000000000000000

Current Network Key: 1

Apply

Setup Wireless – Privacy Page Description

This section describes the section headings and fields descriptions of the Setup Wireless – Privacy page.



If you make changes in the Setup Wireless – Privacy page, click Apply to apply and save your wireless privacy settings.





Field Name	Description
<p>Network Authentication</p>	<p>Network Authentication allows only authorized users to gain access to your wireless network. Only users with an authorized user name, password, or pre-shared key are allowed access to the wireless network.</p> <p>Select from the following Network Authentication protocols:</p> <ul style="list-style-type: none"> • Disabled (factory default) • 802.1x • WPA • WPA-PSK <p> Network Authentication restricts access to your wireless network to only authorized computers or users. Authentication does not protect the data you send over the wireless network connection. You must enable encryption to protect data that is transmitted over your wireless network.</p>
<p>WPA Pre-Shared Key</p>	<p>Allows you to set a WPA Pre-Shared encryption key. Enter a text string in this field. The text string or phrase is used to generate a unique set of encryption keys for your network. Use this string to set up wireless devices in your network.</p> <ul style="list-style-type: none"> • The PSK can be either a text string or a 64 character hexadecimal number. • The text string must be an ASCII character string with a minimum of 8 characters but no more than 63. <p> Not all wireless adapter devices support PSK. For these devices, you must enter the encryption keys exactly as they appear in the in wireless gateway fields in the preceding illustration of the Setup Wireless Privacy page.</p>
<p>WPA Group Rekey Interval</p>	<p>This field sets the WPA Group Rekey Interval in seconds. This only applies when WPA and WPA-PSK Network Authentication is enabled.</p> <p>Set this value to 0 (factory default) to disable periodic rekeying. The valid range is 1 to 4,294,967,295 seconds.</p>

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Field Name	Description
RADIUS Server	<p>Allows you to enter the IP address of the RADIUS server used for authentication and encryption key derivation.</p> <ul style="list-style-type: none"> • This field is used with 802.1x and WPA Network Authentication. • The factory default for this field is 0.0.0.0.
RADIUS Port	<p>Determines the port number of the RADIUS server. The port number is usually 1812 (factory default) or 1645, depending on the server used.</p> <p>This field is used with 802.1x and WPA Network Authentication.</p>
RADIUS Key	<p>This field is used to set the Shared Secret key for your RADIUS connection.</p> <ul style="list-style-type: none"> • The factory default for this field is empty. • This field is used with 802.1x and WPA Network Authentication.
Data Encryption	<p>Allows you to enable data encryption to help secure the data that is sent over your wireless network.</p> <p><u>WEP 128-bit (factory default)</u></p> <ul style="list-style-type: none"> • 128-bit or-64 bit static key data encryption can be selected when the network is configured to have no authentication. • 128-bit static key data encryption is automatically selected when 802.1x network authentication is enabled. <p> Static key authentication uses one of the four encryption keys, as define below, to encrypt your data. You must manually change keys. The keys do not change or rotate automatically as they do with TKIP.</p> <p><u>TKIP</u> (Temporal Key Integrity Protocol) data encryption is automatically enabled when WPA and WPA-PSK network authentication is enabled.</p> <p></p> <ul style="list-style-type: none"> • 64-bit and 40-bit encryption are two different names for the same encryption • 128-bit and 104-bit encryption are two different names for the same encryption
Shared Key Authentication	<p>This field allows you to determine is Shared Key Authentication is used in the network. Shared Key Authentication can be used when there is no other network authentication in the network.</p> <p><u>Optional</u> – (factory default) Wireless clients can associate with the wireless access point without authentication.</p> <p><u>Required</u> – Only wireless clients with a valid network key are allowed to associate with the access point.</p>





Field Name	Description
PassPhrase	<p>A PassPhrase is used to automatically generate WEP encryption keys required to communicate with the network. Although not required for WEP operation, use of a PassPhrase can simplify the configuration and setup of each of your client wireless adapters.</p> <p>Using a PassPhrase eliminates the need to manual enter lengthy encryption keys and reduces the chance of error associated with entering entry of large numbers.</p>
64 Bit Keys 1 through 4	<p>For use with Encryption Mode set to 64-bit encryption. Enter 5-byte values for a Key. You do not have to set all four Keys. Only one Key is used for a home network. Each value is represented in hexadecimal. Use only these numbers or letters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f to set up your encryption keys.</p>  <p>It is generally a good practice to use only lowercase letters when entering WEP encryption keys. Uppercase letters can sometimes be confused with numbers. For example, the uppercase letter "B" is often mistaken for the number "8." Using lowercase characters minimizes the risk of confusing characters when copying keys from one device to another. Uppercase characters will automatically be converted to lowercase when the key or keys are applied and saved to memory.</p> <p>Use two numbers or letters in each box. Record your Key values. You will need these Key values when you set up your client wireless adapter. The Key values in each wireless network device <i>must</i> match.</p>
128 Bit Keys 1 through 4	<p>For use with Encryption Mode set to 128-bit encryption. Enter 13-byte values for a Key. You do not have to set all four Keys. Usually only one is needed for a home network. Each value is represented in hexadecimal. Use only these numbers or letters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f to set up your encryption keys.</p>  <p>The Factory Default setting is 26 zeros: 00000000000000000000000000000000</p> <p>It is generally a good practice to use only lowercase letters when entering WEP encryption keys. Uppercase letters can sometimes be confused with numbers. For example, the uppercase letter "B" is often mistaken for the number "8." Using lowercase characters minimizes the risk of confusing characters when copying keys from one device to another. Uppercase characters will automatically be converted to lowercase when the key or keys are applied and saved to memory.</p> <p>Use two numbers or letters in each box. Record your Key values. You will need these Key values when you set up your client wireless adapter. The Key values in each wireless network device <i>must</i> match.</p>

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Field Name	Description
Current Network Key	<p>Allows you to select which of the four 64-bit or 128-bit keys to use to encrypt your data when you are using encryption that requires the manual entry of an encryption key. Only one WEP key is in use at a time. You must manually change keys. They do not change automatically.</p>  <ul style="list-style-type: none">• 64-bit and 40-bit encryption are two different names for the same encryption• 128-bit and 104-bit encryption are two different names for the same encryption

Function Keys

Generate WEP Keys	<p>Automatically generates four WEP keys based on the PassPhrase entry.</p>  <ul style="list-style-type: none">• For 64-bit WEP, four unique 64-bit WEP keys will be generated• For 128-bit WEP, only one 128-bit WEP key will be generated. The same key will be entered into all four key locations.
Apply	Saves all additions, edits, and changes

Configuring Wireless Data Rates and WiFi Thresholds

Use the Setup Wireless – Advanced page to configure your WAP data rates and wired fidelity (WiFi) thresholds.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default wireless advanced settings.

Click Advanced in the Wireless section of the Setup page to access the Setup Wireless – Advanced page.

Setup Wireless – Advanced Page Example

The following illustration is an example of the Setup Wireless – Advanced page.



We recommend that you do not change the default wireless settings that are shown in the preceding illustration unless you are instructed to do so by your cable service provider.

System **Signal** **Status** **Log** **Setup** WebSTAR Scientific Atlanta

Wireless - Advanced

This page allows you to configure your wireless access point data rates and WIFI thresholds

54g™ Network Mode	Max Compatibility
54g™ Protection	Auto
Rate	54.0 Mbps
Output Power	100%
Beacon Interval	100 ms (0-65535)
DTIM Interval	1 ms (1-255)
Fragmentation Threshold	2346 bytes (256-2346)
RTS Threshold	2347 (0-3000)

Apply

Setup Wireless – Advanced Page Description

This section describes the section headings and fields descriptions of the Setup Wireless – Advanced page.



If you make changes in the Setup Wireless – Advanced page, click Apply to apply and save your wireless advanced settings.


Field Name	Description
54g Network Mode	<p>This setting allows you to optimize the performance of your wireless network.</p> <p><u>Max compatibility (factory default)</u> Allows the access point to interoperate with both 802.11b and 802.11g wireless client devices and minimizes interference with near by 802.11b wireless networks.</p> <p><u>54g Only</u> The wireless access point will only accept 802.11g wireless clients.</p> <p><u>Max Performance</u> Maximum throughput. In this mode, the wireless access point accepts only 802.11g wireless clients. Setting the device in this mode may degrade the operation of near by 802.11b wireless networks.</p>
54g Protection	<p>This setting is used to prioritize 802.11g communication when there is a mix of 802.11b and 802.11g devices in the wireless network.</p> <p><u>Auto (factory default)</u> Maximize 802.11g performance in networks with a mix of 802.11b and 802.11g wireless client devices.</p> <p><u>Off</u> Maximum performance. Networks with 802.11g-only wireless client devices.</p>
Rate	<p>This field can be used to fix the data rate for wireless connections. The following data rates are available:</p> <p>Auto (factory default), 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps</p> <p> In the automatic mode, data rate is a function of signal strength and signal quality.</p>

EXHIBIT A

WebSTAR DPR2320 and DPR2325 Cable Modem Gateway User's Guide

Output Power	<p>This field allows you to adjust the relative output power of your gateway wireless transmitter. The following settings are available:</p> <p>100% (factory default), 75%, 50%, and 25%</p>
Beacon Interval	<p>Displays the time interval that the WAP uses to announce itself to remote devices. The Beacon Interval should be left at 100ms for compliance with most client cards. The Beacon Interval specifies how often packets are sent by the Access Point (AP) to synchronize a wireless network and its clients</p>
DTIM Interval	<p>Displays the time interval between Broadcasts/Multicast transmissions. The DTIM (Delivery Traffic Indication Message) Interval is a countdown informing the wireless clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The DTIM Interval should be left at 3 ms for compliance with most client cards</p>
Fragmentation Threshold	<p>Fragmentation and ready to send (RTS) thresholds should be set equivalent to the maximum Ethernet frame size allowable on the link including overhead (1536 bytes). Lesser settings can damage data throughput as large frames could be fragmented or collisions could occur</p>
RTS Threshold	<p>The RTS/CTS threshold determines at what packet size beyond which the RTS/CTS mechanism is invoked.</p>

Configuring Wireless Access Point Access Control

Use the Setup Wireless – Access Control page to configure your wireless access point access control.



If you are not familiar with the advanced settings detailed in this section, contact your cable service provider before you attempt to change any of the cable modem gateway default wireless advanced settings.

Click Access Control in the Wireless section of the Setup page to access the Setup Wireless – Access Control page.

Setup Wireless Access Control Page Example

System **Signal** **Status** **Log** **Setup** WebSTAR Scientific Atlanta

Wireless - Access Control
This page allows you to configure your wireless access point access control.

Access restriction Closed Network

Access List

Access List is Empty					
----------------------	--	--	--	--	--

Connected Clients
Host Name IP Address

No wireless clients are connected.

0 : 0 : 0 : 0 : 0 : 0

Setup Wireless – Access Control Page Description

This section describes the section headings and field descriptions of the Setup Wireless – Access Control page.

Field Name	Description
Access restriction	<p>When encryption is enabled, this selection allows you to choose one of the following authentication methods from the drop-down list:</p> <ul style="list-style-type: none"> • Open System—Open system authentication allows any device to authenticate and then attempt to communicate with the WAP. Communication occurs if both devices have matching pre-configured WEP keys. Open System authentication does not provide the client with confirmation that the link has been established. This makes it more difficult for a hacker to access the network. • Shared Key—During shared key authentication, the WAP sends an unencrypted challenge text string to any device attempting to communicate with the WAP. The device requesting authentication encrypts the challenge text and sends it back to the WAP. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Shared key authentication provides the client with feedback when a link is denied where Open System authentication does not. • Open System or Shared Key—Either Open System or Shared Key can associate with the WAP and the WAP accepts data from wireless clients using the appropriate form of authentication.
Closed Network	<p>Allows you to disable or enable the network to access by wireless clients. When ON is selected, the access point does not broadcast the SSID. The client device must be configured manually with the SSID and the MAC address of the access point in order to access with wireless network.</p>
Allow/Restrict Access	<ul style="list-style-type: none"> • Disable (factory default) —No access restrictions based on MAC address of wireless access devices • Allow—Allows wireless access to only the MAC addresses listed in the Access List • Deny—Denies wireless access to only the MAC address listed in the Access List

EXHIBIT A

How Do I Configure the Cable Modem Gateway?

Field Name	Description
Access List	Displays the MAC address of the clients that are subject to wireless access control
Connected Clients	Displays the Host Name, IP Address, and Client ID of wireless clients that are connected to (associated with) the gateway modem

Function Keys

The following function keys appear on the Setup Firewall – Event Logging page.

Key	Description
Apply	Applies and saves the values you enter into the fields without closing the screen
Clear All	Clears the Access List
Remove	Removes entries from the Access List
Add	Adds a client to the Access List using the MAC address of the client

Having Difficulty?

Frequently Asked Questions

Q. What if I don't subscribe to cable TV?

A. If cable TV is available in your area, data service may be made available with or without subscribing to cable TV service. Contact your local cable service provider for complete information on cable services, including high-speed Internet access.

Q. How do I arrange for installation?

A. Professional installation from your cable service provider may be provided. A professional installation ensures proper cable connection to the modem and to your PC, and ensures proper configuration of all hardware and software settings. Contact your cable service provider for more information about installation.

Q. How does the cable modem gateway connect to my computer?

A. The cable modem connects to the USB port or the 10/100BaseT Ethernet port on your PC. If your PC is not equipped with an Ethernet interface, an Ethernet card is available from your local PC or office supply retailer, or from your cable service provider.

Q. After my cable modem is connected, how do I access the Internet?

A. Your local cable service provider becomes your Internet Service Provider (ISP). They offer a wide range of services including e-mail, chat, news, and information services. Your cable service provider will provide the software you will need.

Q. Can I watch TV and surf the Internet at the same time?

A. Absolutely! If you subscribe to cable television service, you can watch TV and use your cable modem at the same time by connecting your TV and your cable modem to the cable network using an optional cable signal splitter.

Q. Can I run more than one device on the modem?

A. Yes—a single WebSTAR cable modem will theoretically support up to 253 Ethernet devices utilizing user-supplied Ethernet hubs or routers that you can purchase at your local PC or office supply retailer. Another user at your location can simultaneously connect to the USB port on the cable modem. Contact your cable service provider for further assistance.

Common Troubleshooting Issues

I don't understand the front panel status indicators.

See Front Panel Status Indicator Functions, later in this guide for more detailed information on the front panel status indicator operation and function.

The modem does not register an Ethernet connection.

- Verify that your computer has a 10/100BaseT Ethernet card and that the Ethernet driver software is properly installed. If you purchase and install an Ethernet card, follow the installation instructions very carefully.
- Verify the status of the front panel status indicator lights.

The modem does not register an Ethernet connection after connecting to a hub.

If you are connecting multiple PCs to the cable modem, you should first connect the modem to the up-link port of the hub. The LINK LED of the hub will illuminate continuously.

The modem does not register a cable connection.

- The modem works with a standard 75-ohm RF coaxial cable. If you are using a different cable, your cable modem will not function properly. Contact your cable service provider to determine whether you are using the correct cable.
- Verify that you have followed the procedure in How Do I Renew the IP Address on My PC, later in this guide.
- Your NIC card or USB interface may be malfunctioning. Refer to the troubleshooting information in the NIC or USB documentation.

Tips for Improved Performance

Check and Correct

If your cable modem does not perform as expected, the following tips may help. If you need further assistance, contact your cable service provider.

- Verify that the plug to your cable modem AC adapter is properly inserted into an electrical outlet.
- Verify that your cable modem AC adapter is *not* plugged into an electrical outlet that is controlled by a wall switch. If a wall switch controls the electrical outlet, make sure the switch is in the ON position.
- Verify that the POWER and CABLE indicators on the front panel of your cable modem are illuminated.
- Verify that all cables are properly connected, and that you are using the correct cables.
- Verify that your cable service is active and that it supports two-way service.
- Verify that your TCP/IP is properly installed and configured if you are using the Ethernet connection.
- Verify that you have followed the procedures in How Do I Install the USB Drivers, earlier in this guide, if you are using the USB connection.
- Verify that you have called your cable service provider and given them the serial number and MAC address of your cable modem.
- If you are using a cable signal splitter so that you can connect the cable modem to other devices, remove the splitter and reconnect the cables so that the cable modem is connected directly to the cable input. If the cable modem now functions properly, the cable signal splitter may be defective and may need to be replaced.

How Do I Renew the IP Address on My PC?

If your PC cannot access the Internet after the cable modem is online, it is possible that your PC did not renew its IP address.

Renewing the IP Address on Your PC

Follow the appropriate instructions in this section for your operating system to renew the IP address on your PC.

To renew the IP address for Windows 95, 98, 98SE, or ME systems

1. Click Start, and then click Run to open the Run window.
2. Type winipcfg in the Open field, and click OK to execute the winipcfg command. The IP Configuration window opens.
3. Click the down arrow to the right of the top field, and select the Ethernet adapter that is installed on your PC. The IP Configuration window displays the Ethernet adapter information.
4. Click Release, and then click Renew. The IP Configuration window displays a new IP address.
5. Click OK to close the IP Configuration window, you have completed this procedure.



If you cannot access the Internet, contact your cable service provider for further assistance.

To renew the IP address for Windows 2000, NT, or XP systems

1. Open a Command Prompt (DOS) window.
2. At the C:/ prompt, type ipconfig/release and press Enter. The system releases the IP address.
3. At the C:/ prompt, type ipconfig/renew and press Enter. The system displays a new IP address.
4. To close the Command Prompt window, click on the X in the upper right corner of the window. You have completed this procedure.



If you cannot access the Internet, contact your cable service provider for further assistance.

DPR2320 Front Panel Status Indicator Functions

Initial Power Up, Calibration, and Registration

The following chart illustrates the sequence of steps and the corresponding appearance of the cable modem front panel status indicators during power up, calibration, and registration on the network. Use this chart to troubleshoot the power up, calibration, and registration process of your cable modem.



After the cable modem completes step 7 (Registration Completed), the modem proceeds immediately to Normal Operations. See Normal Operations, next in this section.

DPR2320 Front Panel LED Status Indicators During Initial Power Up, Calibration, and Registration								
Step →		1	2	3	4	5	6	7
Front Panel Indicator		Self Test	Downstream Scan	Downstream Signal Lock	Ranging	Requesting IP Address	Registering	Registration Completed
1	Power	ON	ON	ON	ON	ON	ON	ON
2	Receive	ON	OFF	OCCASIONAL BLINKING	OCCASIONAL BLINKING	OCCASIONAL BLINKING	OCCASIONAL BLINKING	ON
3	Send	ON	OFF	OFF	OCCASIONAL BLINKING	OCCASIONAL BLINKING	OCCASIONAL BLINKING	ON
4	Cable	ON	SLOW BLINKING 1 blink	MOMENTARY ON	OFF	BLINKING 2 blinks	BLINKING 4 blinks	ON
5	PC	ON	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON
6	Wireless	ON	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON

Normal Operations

The following chart illustrates the appearance of the cable modem front panel LED status indicators during normal operations.

Step	8	
DPR 2320 Front Panel LED Status Indicators During Normal Operations		
Front Panel Indicator	Normal Operations	
1	Power	ON
2	Receive	BLINKS – To indicate data is being transferred between the modem and the network
3	Send	BLINKS – To indicate data is being transferred between the modem and the network
4	Cable	ON
5	PC	<p>ON – When a single device is connected to either the Ethernet or USB port and no data is being sent to or from the modem</p> <p>BLINKS – When only one Ethernet or USB device is connected and data is being transferred between the consumer premise equipment (CPE) and the cable modem</p> <p>OFF- When no devices are connected to either the Ethernet or USB ports</p> <p>NOTE: With both Ethernet and USB devices connected to the modem at the same time, when data is being transferred through only one of the devices (Ethernet or USB), the indicator will illuminate continuously. Whenever data is being sent through both data ports (Ethernet and USB) simultaneously, the indicator will blink as described above.</p>
6	Wireless	<p>ON – When the wireless access point is operational</p> <p>BLINKS – To indicate data is being transmitted through the wireless access point</p> <p>OFF – When the user disables the wireless access point</p>

Special Conditions

The following chart describes the appearance of the cable modem front panel status indicators during special conditions to show that you have been denied network access.

DPR2320 Front Panel LED Status Indicators During Special Conditions		
Front Panel Indicator		Network Access Denied
1	Power	SLOW BLINKING 1 time per second
2	Receive	SLOW BLINKING 1 time per second
3	Send	SLOW BLINKING 1 time per second
4	Cable	SLOW BLINKING 1 time per second
5	PC	SLOW BLINKING 1 time per second
6	Wireless	ON or BLINKING

DPR2325 Front Panel Status Indicator Functions

Initial Power Up, Calibration, and Registration

The following chart illustrates the sequence of steps and the corresponding appearance of the cable modem front panel status indicators during power up, calibration, and registration on the network. Use this chart to troubleshoot the power up, calibration, and registration process of your cable modem.



After the cable modem completes step 7 (Registration Completed), the modem proceeds immediately to Normal Operations. See Normal Operations, next in this section.

DPR2325 Front Panel LED Status Indicators During Initial Power Up, Calibration, and Registration								
Step →		1	2	3	4	5	6	7
Front Panel Indicator		Self Test	Downstream Scan	Downstream Signal Lock	Ranging	Requesting IP Address	Registering	Registration Completed
1	Power	ON	ON	ON	ON	ON	ON	ON
2	Receive Data	ON	OFF	OCCASIONAL BLINKING	OCCASIONAL BLINKING	OCCASIONAL BLINKING	OCCASIONAL BLINKING	ON
3	Send Data	ON	OFF	OFF	OCCASIONAL BLINKING	OCCASIONAL BLINKING	OCCASIONAL BLINKING	ON
4	Cable	ON	SLOW BLINKING 1 blink	MOMENTARY ON	OFF	BLINKING 2 blinks	BLINKING 4 blinks	ON
5	Ethernet	ON	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON
6	USB	ON	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON
7	Wireless	ON	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON or BLINKING	ON

Normal Operations

The following chart illustrates the appearance of the cable modem front panel LED status indicators during normal operations.

DPR2325 Front Panel LED Status Indicators During Normal Operations		
Front Panel Indicator		Normal Operations
1	Power	ON
2	Receive Data	BLINKS – To indicate data is being transferred between the modem and the network
3	Send Data	BLINKS – To indicate data is being transferred between the modem and the network
4	Cable	ON
5	Ethernet	ON – When a device is connected to an Ethernet port and no data is being sent to or from the modem BLINKS – When data is being transferred between the consumer premise equipment (CPE) and the cable modem OFF- When no devices are connected to the Ethernet ports
6	USB	ON – When a device is connected to the USB port and no data is being sent to or from the modem BLINKS – When data is being transferred between the consumer premise equipment (CPE) and the cable modem OFF- When no devices are connected to the USB port
7	Wireless	ON – When the wireless access point is operational BLINKS – To indicate data is being transmitted through the wireless access point OFF – When the user disables the wireless access point

EXHIBIT A

DPR 2325 Front Panel Status Indicator Functions

Special Conditions

The following chart describes the appearance of the cable modem front panel status indicators during special conditions to show that you have been denied network access.

DPR2325 Front Panel LED Status Indicators During Special Conditions		
Front Panel Indicator		Network Access Denied
1	Power	SLOW BLINKING 1 time per second
2	Receive Data	SLOW BLINKING 1 time per second
3	Send Data	SLOW BLINKING 1 time per second
4	Cable	SLOW BLINKING 1 time per second
5	Ethernet	SLOW BLINKING 1 time per second
6	USB	SLOW BLINKING 1 time per second
7	Wireless	ON or BLINKING

Notices

Trademarks

Scientific-Atlanta and the Scientific-Atlanta logo are registered trademarks of Scientific-Atlanta, Inc.
DPR2320, DPR2325, and WebSTAR are trademarks of Scientific-Atlanta, Inc.
DOCSIS is a registered trademark of Cable Television Laboratories, Inc.

Other trademarks listed herein are the property of their respective owners.

Disclaimer

Scientific-Atlanta, Inc. assumes no responsibility for errors or omissions that may appear in this guide. Scientific-Atlanta reserves the right to change this guide at any time without notice.

Documentation Copyright Notice

© 2005 Scientific-Atlanta, Inc. All rights reserved.
Printed in the United States of America.

Information in this document is subject to change without notice. No part of this document may be reproduced in any form without the express written permission of Scientific-Atlanta, Inc.

Software Use Notice

The software described in this document is copyrighted and furnished to you under a license agreement. You may only use or copy this software in accordance with the terms of your license agreement.

Firmware Use Notice

The firmware in this equipment is copyrighted. You may only use the firmware in the equipment in which it is provided. Any reproduction or distribution of this firmware, or any portion of it, without express written consent is prohibited.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm between the radiator and your body.

FCC Compliance

United States FCC Compliance

This equipment has been tested and found to comply with the applicable limits of Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or TV reception, which can be determined by turning the equipment off and on. The user is encouraged to try to correct the interference by one or more of the following measures:

- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult your cable company or an experienced radio/TV technician for help

Any changes or modifications not expressly approved by Scientific-Atlanta could void the user's authority to operate the equipment.

The information shown in the FCC Declaration of Conformity paragraph below is a requirement of the FCC and is intended to supply you with information regarding the FCC approval of this device. *The phone numbers listed are for FCC-related questions only and not intended for questions regarding the connection or operation for this device. Please contact your cable service provider for any questions you may have regarding the operation or installation of this device.*

FCC Declaration of Conformity

This device complies with *Part 15 of FCC Rules*. Operation is subject to the following two conditions: 1) the device may not cause harmful interference, and 2) the device must accept any interference received, including interference that may cause undesired operation.

WebSTAR Cable Modem Gateway Model DPR2320 and Model DPR2325 Scientific-Atlanta, Inc. 5030 Sugarloaf Parkway Lawrenceville, Georgia 30044 USA Telephone: 770-236-1077

Canada EMI Regulation

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

For Information

If You Have Questions

If you have technical questions, contact your local cable service provider.



**Scientific
Atlanta**

Scientific-Atlanta, Inc. 5030 Sugarloaf Parkway, Box 565447
770.236.5000

Product and service availability subject to change without notice.

© 2005 Scientific-Atlanta, Inc. All rights reserved.

April 2005 Printed in United States of America

Lawrenceville, GA 30042

www.scientificatlanta.com

Part Number 4003742 Rev B